Montgomery County Government
Enterprise Architecture
Technical Architecture

Department of Technology Services
Montgomery County Government, MD

VERSION	DATE	DESCRIPTION	AUTHOR
1.0	16 March, 2011	Initial version	Mike Tarquinio, Montgomery County Government

Table of Contents

1.0 Introduction

Montgomery County takes advantage of mature technologies in areas of data, voice and radio networking, datacenter operations and monitoring, hardware and software systems deployment, and application development. This document, prepared by the Department of Technology Services (DTS), is part of Montgomery County's Enterprise Architecture. Specifically, this document covers the Technical Architecture.

The Technical Architecture Document reflects key information around the County's Enterprise Technical Domains. It is prepared in concert with the rest of the Enterprise Architecture and the DTS Strategic Plan and is designed to support the initiatives outlined in the plan.

The County has three essential organizational resources, people, process and technology. People are the County's greatest resource, Process binds them together into a coherent workforce, and Technology is the tool.

1.1 Purpose

The purpose of this document is to document key information about the County's Enterprise Technical Domains. Specifically, it identifies the Technical building blocks that are supported in the Enterprise.

1.2 Document Format

The Montgomery County Enterprise Architecture consists of five separate sub-architectures: Business, Technical, Data, Application, and Performance. Each one of the sub-architectures is a standalone document but all five are subcomponents of the entire Enterprise Architecture.

This document addresses the Technical Architecture. It covers the supported Technical Building Blocks or domains at the Enterprise level. Each domain introduces the following topics:

Principles – explaining the purpose of the component, along with some implementation details.

Owners – identifies both the technical and business owners for the component.

Components – expanding on the operational aspects of the component by identifying preferred implementation products and staff skill-sets.

Standards and Guidelines – identifying standards and guidelines which the County follows so that it can provide quality services.

Disaster Recovery – for critical domains this section documents the domain's disaster recovery strategy.

The County has assembled information detailing its technologies and its direction. To avoid releasing potentially sensitive information the county follows a strict release process that involves review at multiple levels (See Section 10-617(g) of the Maryland Public Information Act).

The owner of all five sub-architecture documents and the rollup document is Mike Tarquinio (michael.tarquinio@montgomerycountymd.gov) the Department of Technology Service Enterprise

Architect. The Department is located at the Department of Technology Services, 101 Monroe Street, 13th Floor, Rockville, Maryland 20850.

1.3 Technical Architecture Document Change Management

The Montgomery County Government Enterprise Architecture Technical Architecture document is part of the County's documented Enterprise Architecture and is published by the DTS Enterprise Architect. The Enterprise Architect is responsible for working with DTS Content Experts and department representatives (through TOMG) to document the Technical Architecture. The document adheres to stringent change management controls and follows a defined change management process.

Change requests can be initiated via DTS content experts, TOMG members, or the DTS Enterprise Architect. Contact the DTS Enterprise Architect Mike Tarquinio (michael.tarquinio@montgomerycountymd.gov) for further details.

1.4 References

1. Montgomery County Office of Management and Budget – Administrative Procedure 6-1, June 14, 2004; *Use of the County-Provided Internet, Intranet, and Electronic Mail Services*;

2. Montgomery County Office of Management and Budget – Administrative Procedure 6-6, May 4, 2005; *Information Technology Policies and Procedures*;

3. Montgomery County Office of Management and Budget – Administrative Procedure 6-7, May 4, 2005; *Information Resources Security*;

4. Montgomery County Department of Technology Services, September 2004; *Computer Security Guideline*;

5. Montgomery County Department of Technology Services, 2009; *Enterprise Technology Strategic Plan 2009 – 2012;*

6. Montgomery County Government, May 31, 2007; *Montgomery County Code*;

7. Montgomery County Department of Technology Services, July 19, 2007; *Enterprise Architecture Configuration Management Plan*

8. Montgomery County Department of Technology Services, April 14, 2008; *Montgomery County Government Public Safety Information Technology Architecture*

9. Montgomery County Government; *About County Government*; http://www.montgomerycountymd.gov/mcgtmpl.asp?url=/content/mcginfo/county/welcome.asp; page accessed 3/14/2011

10. Montgomery County Government; *The Charter and County Code*; http://www.montgomerycountymd.gov/mcgtmpl.asp?url=/Content/countyatty/charter.asp ; page accessed 3/14/2011

11. Montgomery County Government; *Montgomery County Organization Chart*; http://www.montgomerycountymd.gov/govtmpl.asp?url=/content/government/aboutgovt/orgchart.asp ; page accessed 3/14/2011

12. Peter Mell and Tim Grance; *The NIST Definition of Cloud Computing*; Version 15, 10-07-09; retrieved from http://csrc.nist.gov/groups/SNS/cloud-computing/;

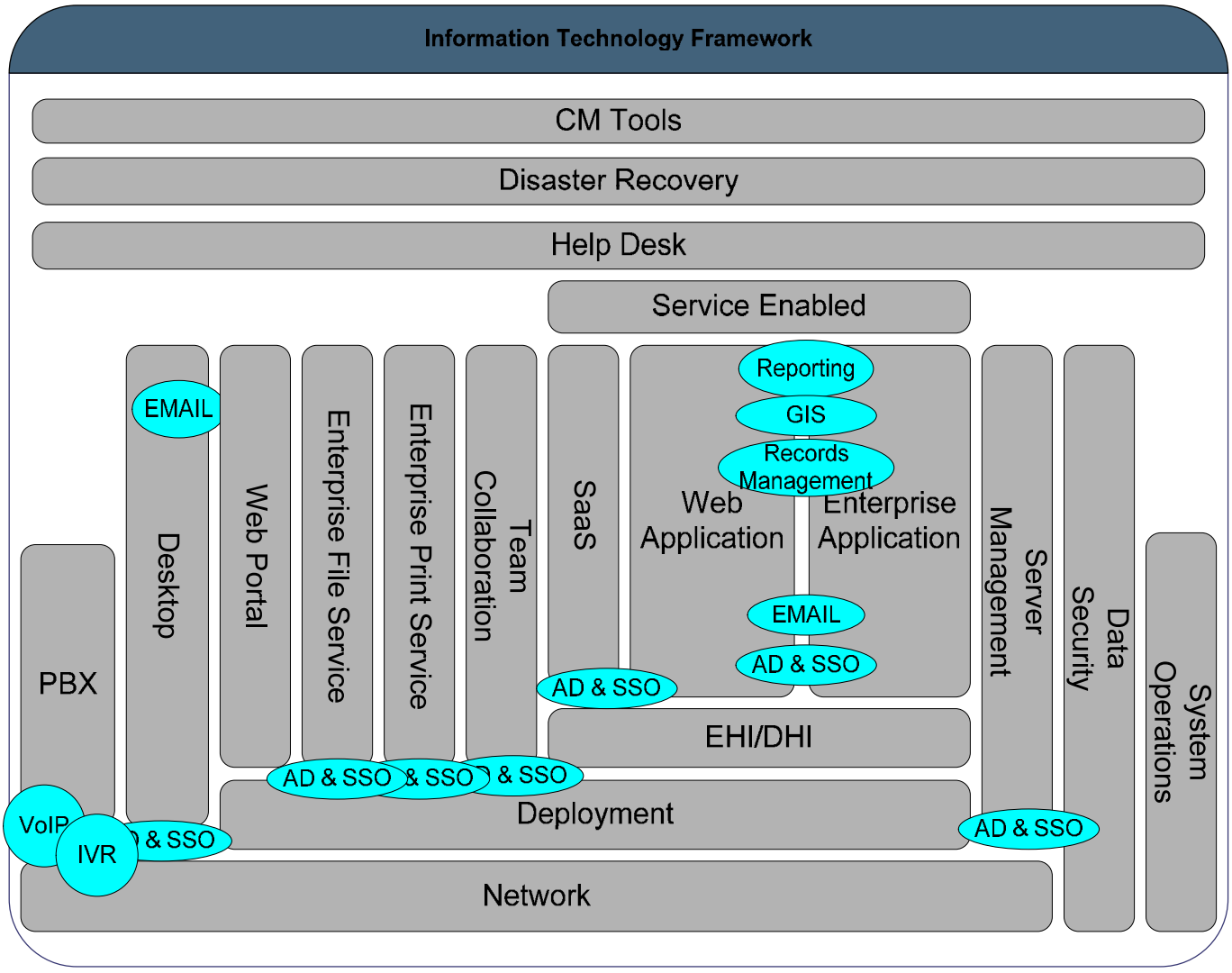
13. Montgomery County Department of Technology Services, March 16, 2011; *Montgomery County Government Enterprise Architecture Business Architecture*;

14. Montgomery County Department of Technology Services, March 16, 2011; *Montgomery County Government Enterprise Architecture*;

15. Montgomery County Department of Technology Services, March 16, 2011; *Montgomery County Government Enterprise Architecture Performance Architecture*;

2.0 Technical Architecture Overview

The Enterprise Architecture presents well-defined, strategic standards adopted for the development and delivery of the County's information systems. It provides a cohesive blueprint to optimally design, purchase, develop, deploy and manage information systems for the County. The components of the overall infrastructure are shown in the next figure:



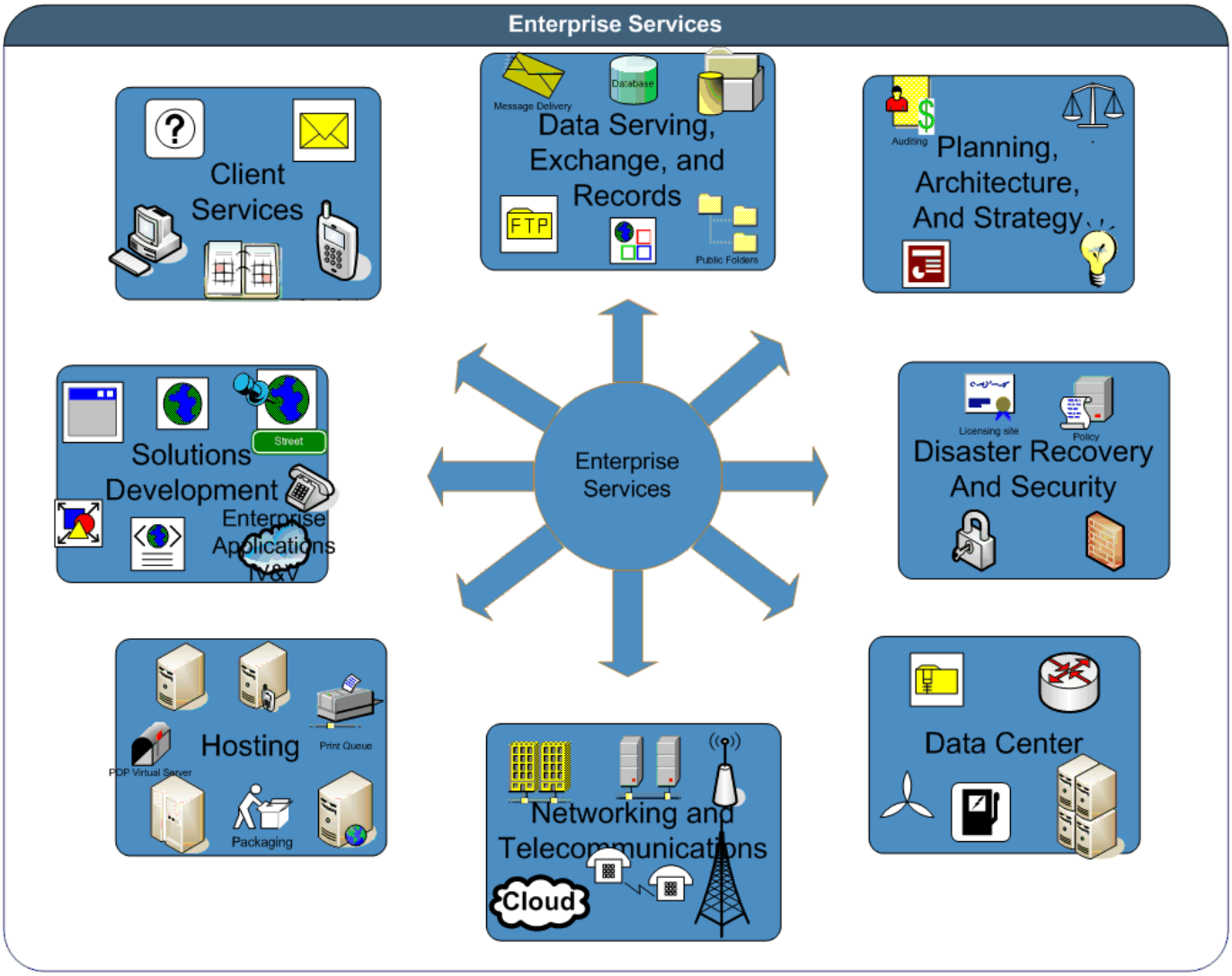
The Framework may be defined as a collection of interrelated component architectures or domains. The public oriented domains are offered as shared Enterprise Services to Departments, Groups, and Agencies and form a Service Catalog. The domains are:

- Active Directory and Single Sign On Services - single enterprise technology directory service that enhances security and efficiency
- Data Security Domain - implementing secure access control management

- Desktop Domain - defining desktop computing standards
- Email Domain - increasing operational efficiencies through a single enterprise email service
- Help Desk - providing assistance to the County
- Geographic Information System – delivering cartographic data and location services
- Record and Document Management Domain - advancing automation
- Reporting Domain – optimizing software licenses and increasing efficiency through a central reporting service
- Enterprise Applications Domain - automating business processes
- Web Applications Domain – developing and deploying applications rapidly
- Service Enabled Domain – avoiding stovepipe applications by supporting standard data exchanges through Web Services and a Enterprise Service Bus.
- Deployment Domain - utilizing resources and sharing costs through standardized servers running as VM Guests on Virtual Hosting Machines.
- Mainframe Application Services Domain - integrating core business processes **(planned retirement - 1/2013)**
- Network Domain - empowering common infrastructure
- Cabling Requirements and Standards Domain- Cabling and wiring standards
- PBX Domain - supplying quality landline services efficiently through an Enterprise PBX
- Interactive Voice Response Domain - integrating IT and Telephony
- Enterprise Hosting Infrastructure Domain - hosting enterprise applications in a secure hosting environment
- Enterprise File Service Domain - centralized shared Enterprise File Service
- Enterprise Print Service Domain - centralized shared Enterprise Print Server
- Database Hosting Infrastructure Domain - database hosting
- System Operations Domain – Enterprise Backup/Data Center Server and Appliance Hosting
- Team Collaboration Domain – providing group collaboration
- Configuration Management (CM) Tools Domain – providing CM Tools Support
- Enterprise Server Management Domain – providing Enterprise Server Management
- Software as a Service (SaaS) – providing support for SaaS applications
- Web Portal Domain – providing Internet and Intranet web portals
- Disaster Recovery - providing IT Disaster Recovery

- Mobile Computing Domain – providing mobile device support

2.1 Enterprise Shared Service Catalog



The public oriented domains are offered as shared Enterprise Services to Departments, Groups, and Agencies and are grouped as follows:

Client Services

- Desktop
- Email
- Help Desk
- Team Collaboration (SharePoint)
- Mobile Device

Disaster Recovery and Security

- Active Directory (AD)
- Disaster Recovery

Hosting

- Deployment
- Enterprise Hosted Infrastructure (EHI)
- Enterprise Print Service
- Software as a Service (SaaS)
- Configuration Management Tools (CM)

Data Serving, Exchange and Records

- Enterprise File Service
- Database Hosting Infrastructure (DHI)
- Enterprise Service Bus (ESB)
- Record and Image Management

Networking and Telecommunications

- Network
- PBX
- Cabling Requirements and Standards

Data Center

- System Operations (Enterprise Backup/Data Center Server and Appliance Hosting)
- Mainframe Operations

Solutions Development

- Geographic Information System (GIS)

3.0 Architecture Domains

3.1 Active Directory (AD) and Single Sign On (SSO) Services

Principles

Microsoft's Active Directory (AD) is used to authenticate users, and to allow them into the County network. Single Sign On (SSO) services is an enterprise strategy designed to minimize administration and user authentication stress, eliminate multiple userids and multiple passwords. The Single Sign On service is implemented through Tivoli Access Manager (TAM) and Active Directory. With AD and TAM, users are able to log on to the network, and log into specific SSO configured applications as the need arises. For example, once the user is logged into the network, the user is not required to log into Exchange to access the County's email system.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

Active Directory is built around a number of Active Directory servers strategically located throughout the County government (see figure 3-1). If a failure should occur, having multiple servers increases the potential for employees to authenticate into the network. The system design allows for all servers to replicate on change, with the exception of one. The one non-synchronized server is an emergency backup copy used for recovery, and it replicates once every 24 hours.

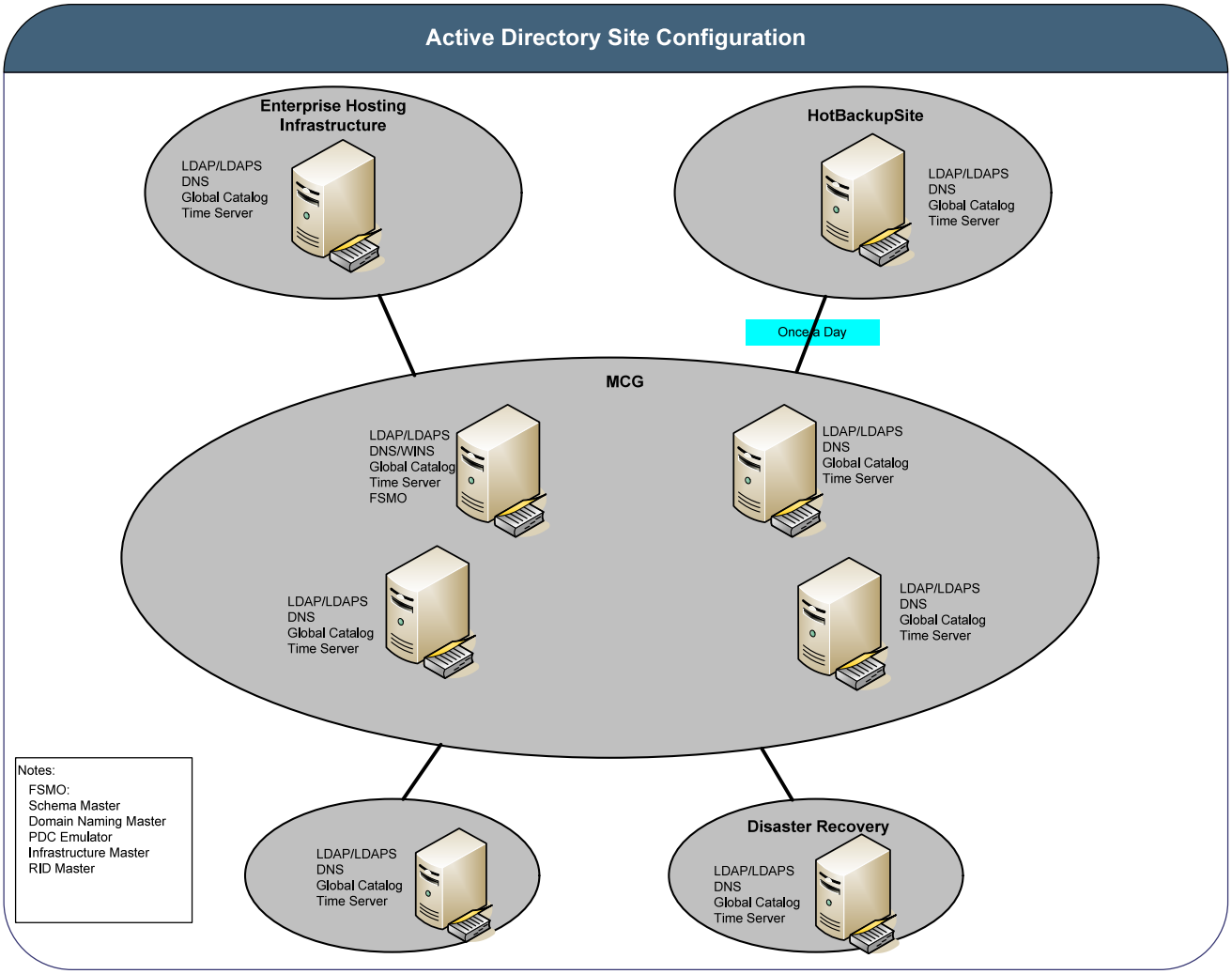


Figure 3-1 AD Site Configuration

The Department of Technology Services (DTS) manages the Enterprise Directory structure and group policies. DTS is the sole Administrator at the Enterprise level and delegates the management of select OU admin functions to department administrators. Each department's resources is defined and contained inside their own OU. Department OU Administrators have the responsibility to add, delete, and modify accounts within their OU, and to set permissions for their departmental applications.

Departmental Applications that are hosted within the DTS Enterprise Hosting Infrastructure (see section 3.7 - Enterprise Hosting Infrastructure) have permissions setup for each by DTS Administrators. DTS creates one or more Application OUs for each application and gives owning department administrators the ability to assign users to the Application OUs. When authenticating into one of these applications, TAM acts as a clearinghouse front end to AD, checking AD permissions as the user logs on. Each County employee has an account in TAM which allows for SSO application use.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Active Directory Domain Administration
Windows Server Administration
TAM User Account creation
Understanding of Security Principles
Ability to use Magic Help Desk System
DNS, WINS and DHCP Administration

Standards and Guidelines

Special Root or Organizational Units (OU) Folders have been created to provide for additional functions in our environment, and for application SSO management. These are as follows.

Department OU Folders – Each County department is designated a specific OU folder to administer their department Users, Computers, Resources and Groups. The names assigned are based on the standard acronyms used for each department. If the department does not have an OU Administrator, DTS assumes the responsibility.

Department Servers Folders – Each County department is designated a specific OU folder to administer their departmental servers.

Applications - OU is used for SSO. Each County SSO application is assigned a sub-folder under this OU. Groups are created and assigned rights for these applications.

Associates – OU is used for SSO and Associates. These are Non Mail Enable Accounts (NME). The OU is made up of two sub-OUs; former County employees, and non-County or former employees who need access to SSO applications. This is for groups like the Howard county police who need access to the Auto Theft Application, employees in sister agencies, boards and committees requiring access to Financial Discloser, or former employees needing access to benefits or deferred comp.

Computers – This is a default OU created by AD. Computers that are not pre-staged are added to the domain here. Domain admin authority is required to move these computers into their appropriate department OU.

External Contacts – This OU houses external contact information (name and external email address) in a centralized location. This allows the departments to create standard email distribution lists that include external email contacts. This process is primarily in place to overcome the limitations of Outlook for distribution lists. It is managed by the Core System's group in DTS.

Inactive – This folder has three sub-OUs; Retired, Terminated and Survivor. This folder contains

former employee accounts that have been deactivated and their mailbox removed. These former employee accounts are being saved because in the near future they will need to have access to various SSO applications such as retirement and insurance benefits.

Training – OU for Admin, Power User, Svr Training. Server Admin holds user accounts which are disabled. These are accounts that probably will not be used again, but we don't want to have to recreate them. Two other OU folders contain accounts used for OU admin, Outlook, and other types of training.

Test – This folder is kept at the root, for easier access to other departments. Usually used only by Domain Admins, it is used to test policies, or to replicate issues the users may have with external contacts, etc.

Training

All Department OU Administrators must attend the DTS OU Administrators training class prior to performance of Administration functions.

Standards

PC Policies for Improved Security & Manageability

- This policy uses AD to lockdown PCs and maintain standard configurations

The Enterprise Directory is a non-federated service

3.2 Cabling Requirements & Standards

Principles

The County's goal is to standardize its cabling infrastructure to promote faster speed, better communication, easier troubleshooting, and less need for repair. DTS Telecommunications offers connectivity for telecommunications equipment throughout the County. Cable installation services are offered by the County and by outside Contractors.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS PBX Telephone Service Team.

Components

The County's telecommunications systems are interconnected by various cables. The County's cabling infrastructure contains a wide variety of cables including the County standard Category 5e and 6 (Cat-5e and Cat-6) cabling. Cat-6 cabling is the latest addition to the County's structured cabling standards, and it has twice the bandwidth of Cat-5e cabling for improved service.

Standards and Guidelines

The County Cabling standards and guidelines are for vendors and County departments which install and support the County's cabling infrastructure. As universal standards evolve, the current standards and guidelines will be updated in this document. The County maintains a standards document located at the following location on the County Internet portal -

http://www.montgomerycountymd.gov/dtstmpl.asp?url=/content/dts/architecture/services/CablingDomain/index.asp

3.3 Data Security Domain

Principles

Security is an essential part of every component in the County's IT Architecture framework with multiple domains and groups having responsibilities. The Security Domain includes not only technology but process and procedures and is present through all aspects of system acquisition and development.

The following domains have Security responsibilities:

- Active Directory and Single Sign On – Centralized Directory Service supporting Single Sign On Services
- Deployment Domain – Common Enterprise Server configurations and patch management services
- Desktop Domain – Centralized desktop management with common configurations, patch management services, lockdown policy, centralized anti-virus and anti-spyware services
- Email System Services – Centralized mail service including anti-virus, anti-spyware and spam removal services
- Enterprise Hosting Infrastructure – Secure hosting infrastructure
- Help Desk Services – Centralized help desk that supports Incident Response
- Network Domain – Enterprise network that includes protected single point of access, internal and external firewalls, wireless security, and network segmentation services
- Service Enabled Domain – Use of an Enterprise Service Bus for centralized secure information transfers
- System Operations Domain – Centralized Data Center that includes redundant systems for high availability and physical security measures
- Configuration Management – Centralized Configuration Management systems for protection of project assets.
- Enterprise Server Management – 24x7 server monitoring
- Security Domain – Includes policies and procedures, risk management practices, Virtual Private Network access, and operational security monitoring including security scanning, policy enforcement, and log correlation.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Security Team
- DTS Core Systems Team
- DTS Server Team
- DTS Client Computers (DCM) Team
- DTS Network Services Team
- DTS Data Center Operations Team

- DTS Help Desk Services

Components

In addition to the Security components in use within each of the various domains mentioned in the Principles Section the following additional Security components are in use:

- Log Correlation
- Intrusion Detection
- Web Filtering
- Port and Vulnerability Scanning
- VPN
- Anti-Virus and Anti-Spyware protection
- Laptop Encryption
- Computer Security Investigations

Log Correlation

The DTS Security Team maintains a centralized log correlation system that monitors critical IT Components within the county.

Intrusion Detection

The DTS Security Team maintains an intrusion detection system that monitors critical parts of the County Network.

Web Filtering

The DTS Security Team manages a Web Filtering system that manages employees' use of the Internet. It has the ability to block, permit, limit by time-based quota, or postpone access to individual categories by user, group, workstation, or network.

Port and Vulnerability Scanning

The DTS Security Team uses various port and vulnerability scanning tools to scan the network internally and externally.

VPN

The County's VPN solution authenticates users, encrypts data, and provides flexible access controls for client-to-application security. With the current solution, the County can securely share critical information and applications with employees and business partners via the Internet. The VPN provides centralized access into the County network for employees and validated contractors. No other method is allowed.

Anti-Virus and Anti-Spyware Protection

The County uses centralized Anti-Virus and Anti-Spyware Protection software to provide scalable, cross-platform virus protection for workstations and network servers. County workstations and servers are currently checking for updated virus signatures every 60 minutes. This "normal conditions" deployment was architected to minimize the response time and increase the effectiveness of signature updates to all County hosts. In emergency situations signatures will be pushed out immediately to limit the County's

exposure to virus, worm, and Trojan activity.

Laptop Encryption

Because of various regulatory compliance initiatives and the due diligence obligation to the citizens of Montgomery County, the DTS Client Computers (DCM) team supports a hard disk encryption solution for mobile users. The purpose of the solution is to make all data on the hard drive unreadable should a laptop become lost or stolen. All primary county laptops must be encrypted.

Computer Security Investigations

The DTS Security Team provides Computer Security Investigation services.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Network Administration – Routers, Firewall, VPN, Protocols
Network, Server and Desktop Administration. Installation and Troubleshooting.
WAN Hardware Management
IDS Administration, Penetration Testing, Vulnerability Assessment and Remediation. Forensic analysis Exploitive techniques: exploit coding, virus reverse engineering and analysis, packet crafting, various injection techniques

Standards and Guidelines

Governance

- Office of Management and Budget – Administrative Procedure 6-1 *Use of County-Provided Internet, Intranet, and Electronic Mail Services*
- Office of Management and Budget – Administrative Procedure 6-6 *Information Technology Policies and Procedures*
- Office of Management and Budget – Administrative Procedure 6-7 *Information Resources Security*
- Office of Management and Budget – Administrative Procedure 8-2 *HIPAA Compliance and Responsibilities*

Policies

- Help Desk (see section 3.9 - Help Desk Services) provides central point of contact for incident response
- PC Policies for Improved Security & Manageability (see section 3.1 - Active Directory and Single Sign On (SSO) Services and section 3.5 – Desktop Domain)
- Montgomery County Government Department of Technology Services – EID Incident Response Plan; DTS Security Team
- DTS Security Team Risk Assessment Policy

Education

- County Security Awareness training

Incident Response

- Perceived or actual security incidents must be reported immediately to one of the following:
    - CIRT Lead/Security Official
    - DTS Security Team
    - IT Help Desk at 240-777-2828
    - Department Head
    - Department IT Staff

3.4 Deployment Domain

Principles

The Deployment Domain is an Enterprise VM Guest Hosting Service that meets 4 of the 5 essential characteristics of the NIST definition of Cloud Computing [12]. The 4 supported tenants are: Broad Network Access, Resource Pooling, Rapid Elasticity, and Measured Service. The one characteristic that is not supported is On-demand Self-Service which the DTS Server Team intentionally reserves internally. The Deployment Domain is providing private cloud services to County departments and agencies.

The Domain consists of standardized server hardware, operating systems, middleware and personnel. The DTS Server Team provides standardized VM Guest instances to requesting departments or groups. The requesting departments or groups can use the VM Guests to run their own applications. The DTS Server Team manages the VM Guests and runs them on a farm of VM Hosting machines that they solely control and administer. The use of the standardized building blocks allows a standard set of services to be provided by the DTS Server Team. Such services include standardized backup, monitoring, problem avoidance, dynamic configuration, and patch management.

The Deployment Domain makes use of the following Enterprise Architecture services:

- Enterprise Server Management (providing 24x7 monitoring)
- System Operations Domain (providing data center hosting services - power, air conditioning, 24x7 facilities monitoring, etc)
- System Operations Domain (weekly tape backup services)

The goals of the Deployment Domain are to:

- Provide robust and stable IT environments.
- Maintain a continual pool of spare server capacity, which can be used for new deployments, horizontal scaling and sparing.
- Provision new server and middleware environments in near real time.
- Research and adopt new tools and building blocks to lower Total Cost of Ownership (TCO).

Successful operational procedures include:

- In-house web mastering of technical documentation and dashboards.
- Routine auditing and upgrading of system patch levels, anti-virus engines and backups.
- Automation of routine operations and monitoring.
- Detailed peer reviews prior to new deployments.

Deployment Zones

When a VM Guest is configured it can be inserted into one of 3 standardized deployment zones. Each zone is tailored for a specific set of users and security rating. For example, the Enterprise Hosting

Infrastructure (EHI) is for internal users. More specifically, the EHI only supports users who are in the County's Active Directory system.

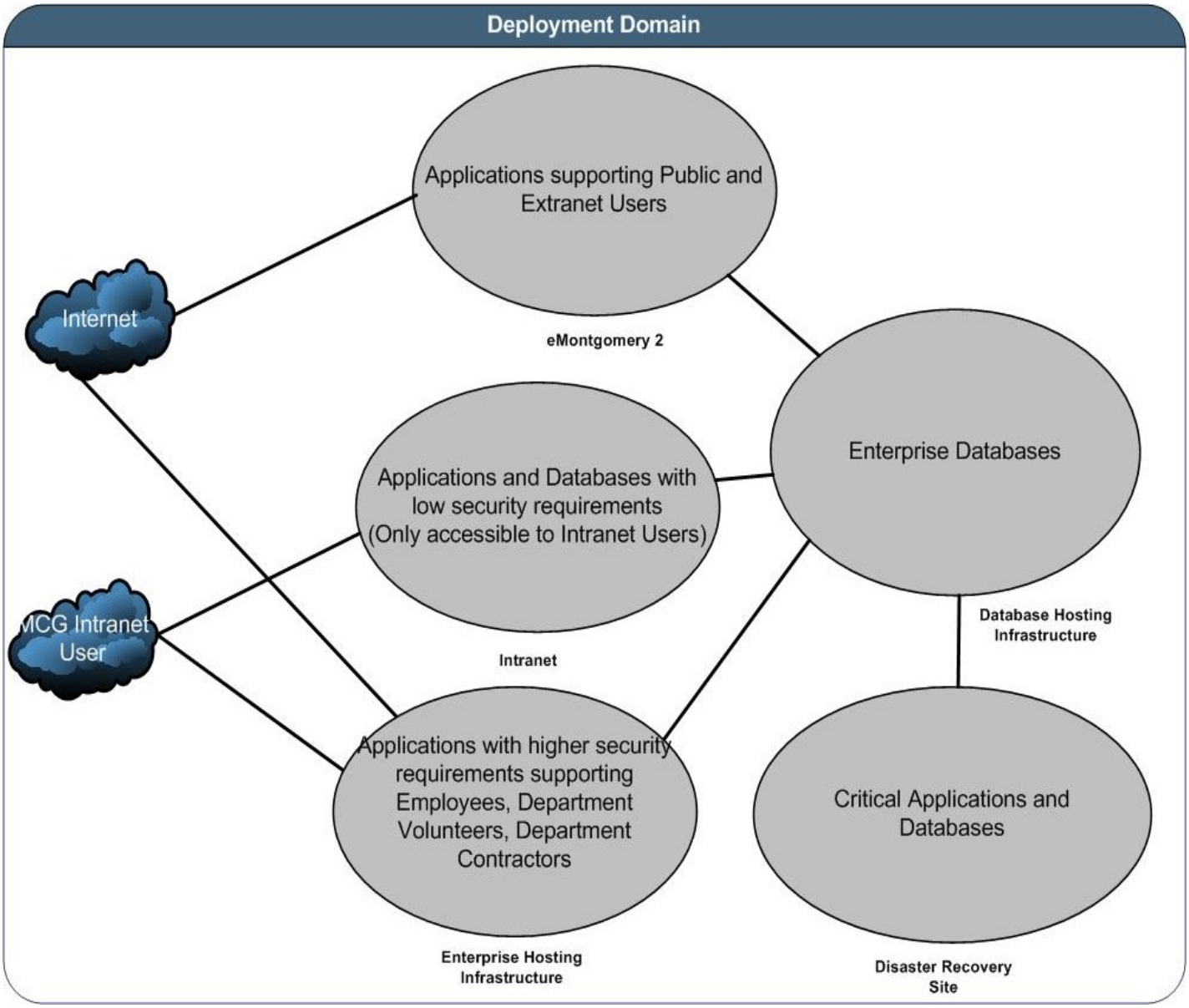


Figure 3-2 Deployment Zones

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Server Team

Components

Hardware

The County has standardized on Dell x86/x64 midrange rack mount servers, which are configured at the high end of memory and disk capacity.

Hardware Capacity Planning

A sliding window of funding and replacement cycles is used for server capacity planning. New GENERATION N and N-1 servers are typically deployed as VM-HOST or DB servers. GENERATION N-2 servers released by the renewal process can become standalone servers. This process is followed a high percentage of the time for enterprise servers.

The following benefits are realized:

- Elimination of hardware selection, sizing and procurement delays
- Identical servers are purchased within a GENERATION.
- Horizontal scaling and/or VMs are used to meet processing requirements.

For example, instead of procuring 3 small servers for 3 projects, in-place capacity is used via VMs. New VM-GUESTS (for the projects) are provisioned in real-time. Project funding, from the 3 projects is lumped together to purchase a new GENERATION N server which adds back additional capacity.

Speed and ease of new server deployments

Most new servers take on the role of a VM-HOST. In just a few hours time, these servers can be activated because only the OS, the VM engine and the utility software need to be installed. VM-GUESTS (new or existing) are then activated. Typically, this is a copy/paste operation.

Hardware maintenance savings

GENERATION N servers typically come with a 3 year warranty. There is no maintenance cost during this period. Once out of warranty, there are sufficient “spares” to cover production failures. “Time and Materials” is used to cover repair expenses once out of warranty.

Operating System, Database and Middleware

The county stays current with Operating System and Middleware versions. The following table outlines typical versioning. Most components have service pack upgrades throughout the year with version upgrades every couple of years.

1.

FUNCTION	COMPONENT VERSION	OS VERSION
WEB/APP SERVER J2EE	JBOSS	CENTOS

Web/App Server Microsoft	ASP .NET	Windows Server

Table 5-2

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Area	Skill Set
OS	Linux (CENTOS) , Windows Server
DB	MS SQL Server, Oracle Server
Middleware	.NET AD ASP IBM MQ Series ESB (MULE) IBM Tivoli Access Manager (TAM) J2EE /JBOSS
Operational Support	Shell Scripting/ Perl Webmastering JUnit/HTTPUnit JMX
CM	SVN and TRAC
Other	Technical Project Management

Standards and Guidelines

- Current availability guideline is to keep system components available 99.5% of the time.
- DTS solely has access and manages the VM Hosting Servers.
- Outage reports through HelpIT updates
- Maintenance window announcements through HelpIT updates
- County has standardized on Dell x86/x64 midrange rack mount servers, which are configured at the high end of memory and disk capacity.
- County stays current with Operating System and Middleware versions. Most components have service pack upgrades throughout the year with version upgrades every couple of years.

Disaster Recovery

The Deployment Domain involves the use of VM Guests running on VM Hosting Servers housed in the Data Centers in the System Operations Domain. A number of disaster recovery strategies in the Deployment and System Operations Domains are employed that essentially cover the following disaster scenarios:

- server loss
- rack loss
- data center loss

The server loss and rack loss strategy has a number of mitigation strategies within the System Operations Domain. Within the Deployment Domain the mitigation strategies include:

- use of VM Guests as well as pooled VM hosting machines located in both data centers.
- in the event of individual server or rack failure critical VM Guests will be moved to working VM hosting machines
- in the event of a data center failure critical VM Guests will be moved to working VM hosting machines in the other data center.

The design problem for the loss of one of the Data Centers is the prioritization of services that will be brought up in the working data center. See section 3.23 Technical Disaster Recovery for information around prioritization of services and policies.

3.5 Desktop Domain

Principles

Desktop Computer Modernization is a centralized program for the planning, acquisition, asset management, and support services associated with desktop computers. Desktop Computer Modernization (DCM) is part of the Department of Technology Services (DTS). Under this program, the County uses its own in-house personnel for integrated desktop planning, and a single external service provider for desktop acquisition assistance, asset management, and support services. Through the implementation of DCM, the County achieves several key goals:

- Brings current technology to the desktop
- Reduces the cost of and need for support services through planning
- Provides a single source of support through a centralized single point of contact IT Help Desk
- Provides quality services to end users in an accurate, consistent, timely and professional manner
- Controls total cost of ownership.

The DCM program covers the primary seat machine for the individual worker. DCM supports based on user requirements and support considerations non-traditional as well as traditional desktops. Supported desktops include various configurations of the traditional desktop as well as laptops, netbooks, and tablets.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Client Computers (DCM) Team.

Components

Desktop Environment

The County currently has approximately 9600 primary PCs and laptops which are located throughout the County. Existing computer equipment consists of DELL and Lenovo business class systems. The County has a 4-year replacement cycle for primary systems, subject to funding restrictions. Generally one fourth of the County's current base of PCs is replaced each year.

External Service Provider

DCM has a single external service provider for all help desk and desktop support, asset management and computer acquisitions. DCM's current external service provider maintains a location approximately one mile from the Rockville Core which has a warehouse facility. This is also the location of the centralized IT Help Desk (see section 3.9 – Help Desk Services).

Asset Management

Computer hardware inventory is maintained by the external service provider in a SQL based application. The external service provider is responsible for maintaining accurate inventory reporting and continual data validation. The DCM program office staff has direct access to this database. The external service provider also makes Department inventory reports available through the intranet.

Desktop Management

DCM maintains the County's Systems Management Server (SMS) Enterprise system and database. SMS allows for a central point of desktop management, software deployment, and remote control of desktops and laptops throughout the County. The County also uses Shavlik as a patch management tool to deploy Microsoft OS security updates. This tool is managed by the external service provider.

Disposal of Equipment

DCM provides the County a mechanism to dispose of old computer hardware through its external service provider. Before a system can be disposed, the external service provider wipes all data from the hard drive(s) using software and procedures that meet DOD certified sanitization standards. Computer systems are then disposed or remarked in a manner that meets environmental standards. This process ensures the removal of all data from system hard drives and provides the County with the ability to maximize residual value on assets.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Project Management and Contract Administration
SMS Administration and Application Development
Wise Studio Scripting Language
SQL Administration and Maintenance
Windows Server
Microsoft Desktop OS/Platform
Dell & Lenovo Business Class Hardware
County Core Applications including MS Office, Outlook, Internet Explorer, PComm, Adobe Reader, Sophos
Networking and Basic Active Directory

Standards and Guidelines

The current DCM Program Team is responsible for PC lifecycle planning and managing desktop services provided by the external service provider. The external service provider is responsible for acquisitions of new desktop equipment; imaging systems using configurations provided by DCM staff that meet current County and Security standards; help desk and deskside services; computer maintenance and repair; and asset management.

Planning
The DCM program develops and maintains a comprehensive plan covering the life cycle of the County's PCs; integrating all aspects of desktop acquisition; help desk support; and asset disposal. The DCM program focuses on reducing the need for maintenance and other support services, while also planning for changes in technology and the IT industry. This includes developing a desktop deployment strategy and enterprise wide desktop software roll-outs (operating system upgrades, software installations, patches and new applications). The DCM Program also maintains detailed schedules identifying the PCs to be replaced, moved, installed, upgraded, disposed of, or redeployed. Planning for replacements simplifies the acquisition process by ordering in advance, minimizing disruptions to County users, providing a steady workflow, and reducing costs.

Standards

Establishes enterprise-wide standards for hardware, software, and supporting processes. DCM also standardizes on several desktop, laptop, netbook, and tablet configurations used throughout the County. A list of optional add-ons to the standard configurations is available to end-users as required.

Budgeting

Forecasts and manages desktop budget. Collects and analyzes the total cost of desktop equipment and services, reducing the total cost of ownership.

Acquisition

Functions as a single point of contact with vendors for scheduling, and obtains all desktop equipment (places orders; tracks status; approves and processes invoices).

Asset Management

Centrally manages the County's desktop and laptop assets to maximize the return on investment. Directs the external service provider to update and maintain inventory information in the asset management database. Defines the web based reports the external service provider maintains on the intranet for Department inventory.

Contract Administration and Coordination

Oversees all DCM activities, and coordinates the resolution of escalated incidents. Monitors contract service levels in accordance with the current DCM contract. Defines and reviews monthly management reports and real-time dashboards prepared by external service provider Contract Administration functions as a single point of contact.

Security Standards

PC Policies for Improved Security & Manageability

- This policy uses AD and SMS to lockdown PCs and maintain standard configurations

3.6 Email System Services

Principles

The County uses Microsoft Exchange for its enterprise email system. This system supports Enterprise wide email functions to employees within the County and locations anywhere around the world. Access is allowed via the Outlook desktop client, Outlook Web Access (OWA) web browser, Blackberry and other ActiveSync supported devices. Mailbox stores are managed centrally, and backed up at the server level (not at the brick level). Administration is both centralized and decentralized depending on the specific department and need. Anti-Spam processing and filtering for both inbound & outbound mail is supplied by two Spam Protection Appliances.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

The email system consists of a number of back-end Exchange servers and one hot spare server. The hot spare server also serves as a production test server. Each server supports an average of 2600 mailbox accounts. Two front-end, OWA servers provide web access for more than 85,000 sessions each week. The servers support all of the versions of the Outlook client, but the County standard is currently Outlook 2002 and 2003.

Spam protection is provided by two Spam Protection Appliances. They process nearly 2,000,000 inbound and outbound messages, while blocking or deleting an average of 1,100,000 spam messages each week. These two servers provide a “first line of defense” against spam. They perform white listing (allowing specific messages thru), black listing (blocking messages from domains and specific addresses), and use sophisticated algorithms to filter and remove 80-90% of all inbound spam. An anti-virus scanning engine scans all of the messages and message stores for viruses. Other features include attachment blocking, and file quarantine of known executable and dangerous attachments.

Two mailbox servers are configured as default SMTP Virtual Servers, routing mail in and out of the Spam Protection infrastructure for Montgomery County employees. Another Exchange mailbox server is configured with a virtual IP address and is used to route mail from non Exchange server messages and perform as a relay agent for internal messages generated outside of the Exchange servers.

Users authenticate to Exchange via Microsoft Active Directory (AD). Accounts and other Active Directory components within the Departmental organizational unit are administered by local Organizational Unit (OU) Administrators for most departments. Enterprise Administrators support the remaining departments and support all OU Administrators. User accounts are published in the Global Access List (GAL) which allows employees to easily lookup addresses, locations, departments, and phone numbers from within Outlook. Email accounts can be classified as employees, interns, contractors, volunteers, or temporary.

Enterprise level administrators can create Contacts so that non-County partners, and contacts with non-County email addresses, can be published in the GAL allowing for membership in groups and easy emailing. The system also handles resources and conference rooms, providing scheduling services at the department and enterprise level.

Blackberry devices are supported at the enterprise level. User departments purchase the units, and contact DTS to purchase server client access licenses (CALs). The user departments then call the Help Desk to configure the device software on the desktop. Either the Help Desk or the employee opens a Magic ticket for Core Systems to configure the device for wireless activation. The current software also allows for wireless activation (so at account creation, the account can be activated for the user versus having the Help Desk or OU admin perform the synchronization and activation from the desktop. Devices running version 4.x and above no longer require the Blackberry to be docked to receive additional software products. However the client device software must be installed on a desktop in order to support device software upgrades.

DTS has tested other devices such as the Android, iPhone, Windows mobile phones, etc. Although they have the ability to connect and synchronize (at various levels of effectiveness), they are not at an enterprise level of stability and manageability, that the Blackberry devices are. Therefore, we will continue the policy of providing enterprise support for Blackberries only. The County will allow, where security is not compromised, connectivity of non-Blackberry devices to the Exchange system. Requests for issuing/connecting a non-Blackberry device will be referred to the employee's Department OU administrator for action. The Departments will determine whether to issue/connect non-Blackberry devices and will be responsible for setup and providing support for the non-Blackberry devices.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Microsoft Active Directory Administration
Microsoft Exchange Administration
Magic Help Desk System
Server, Network and Messaging Security
Windows Server Administration
Good Communication Skills
Systems Management Server (SMS)
Knowledge of email processing and types of email
Knowledge of Spamming methods, and remediation
Anti-Virus Administration
Wireless Email Administration
Knowledge of Virus propagation and methods of prevention and removal
Knowledge of eMessaging Standards and enforcement methodologies
Anti-Spam Server Administration Skills
Knowledge of the Outlook Client and features

Standards and Guidelines

Availability/Uptime: The system is designed to be available 24/7 with the exception of a 4 hour maintenance window on the Friday following the 2nd or 3rd Tuesday of each month. This time is for routine or critical maintenance and software installations. This creates an uptime goal of approximately 99.5%.

A single enterprise email address standard:

FirstName.LastName@montgomerycountymd.gov

There is an eight character minimum. Those accounts with less than eight characters will receive x(s) to meet this requirement. To eliminate duplication, FirstName and the addition of middle initial can be used.

Specific naming conventions have been defined for Distribution Groups, Resources, Rooms, Non-Fixed resources

Shared mailboxes are defined at the enterprise level, and managed at the OU level

USERID/Mailbox policies

Deletion

Enterprise Core Systems team will monitor the use of mailboxes, and departments will be notified of mailboxes not accessed in last 60-90 days. After 90 days not being accessed, mailboxes will be deleted.

Each Dept/OU Administrator must establish an internal procedure to remove mail boxes. When an employee is terminated, the AD accounts must be deactivated **ON THE SAME DAY.**

If a department needs a mailbox, it must be copied to a PST file and saved separately.

If a department needs to temporarily access a de-activated account, the password must be reset to limit potentially damaging access by the former employee.

Once the department is finished with the employee account and it has been de-activated, the account must be deleted (as in the case of a temp, intern or contractor account) or moved to the AD Root folder INACTIVE folder (as in the case of a Retired or Terminated account).

Mail

Duplicate email addresses cannot exist.

Resources can be mailbox enabled.

Department distribution groups should use an Access Control List (ACL) to limit other department's access. Options should be set to "disallow with exception".

Global Distribution groups will be created by the Core Systems team at the enterprise level.

Users are limited to sending emails to a maximum of 2000 recipients unless special permissions are granted.

Address List

Global Addresses

All users, groups, contacts, conference resources & public folders

Department address list

All employees

Department employees

Mail Store

Each dept has a designated mail store, for example, the mail store for the Board of Investment Trustees is BIT1. The number indicates the number of mail stores for the group.

Enterprise Exchange Administrators will monitor capacity and notify departments when allocations are reaching maximum limits.

Sirana AppAnalyzer can be used to monitor the overall system and individual mailbox capacity, and email traffic.

Exchange is configured to check capacity every 4 hours.

Calendar

Currently the County's standard is for 2 months of Free/Busy schedule publishing, special use calendars, and conference room calendars. In the future we may wish to publish a recommended 6 months.

Personal Address Books (PAB)

Not supported at the enterprise level

Individual Mailboxes

The system is designed to handle 10,000 mailboxes at 1000 MB each.

Local storage policy (private folder) will be determined by each department.

Administratively deleted mailboxes will be retained for 10 days. For mailbox recovery, contact DTS through the help desk.

Individually deleted items (messages) can be recovered up to 24 hours after deletion. For recovery instructions contact the Help Desk.

Each mailbox limit set to 50MB. Requests for temporary or permanent limit increases must be sent to the Help Desk. Each request will be reviewed on its specific merits. In most cases, decisions will be made on the same day.

When they login, users will be warned when storage reaches 45MB

Users will be prevented from sending messages when storage exceeds 47MB in size.

Users will be prevented from receiving messages when storage reaches 50MB in size.

All messages (including attachments) are limited in size to 10 MB.

Outlook Client's Deleted Items folder will be emptied at logoff, but items will be recoverable for up to 4 days.

SMTP access for County Applications requiring outbound mail support via mcg-relay.mcgov.org

No POP or IMAP protocol support.

Email Administration is done in the Departments through Active Directory Departmental OU

Administrators (see section 3.1 Active Directory (AD) and Single Sign On (SSO) Services)

Backup/Restore

DTS backs up Email servers for disaster recovery purposes. DTS' current recovery process is to restore servers in the event of system crashes, facility loss, or some other disaster. To support the current model, the Email System Service Domain uses the backup services of the System Operations Domain (see section 3.17 System Operation Domain). Refer to that domain for backup retention times.

Email administrator requested restoration of individual items is limited by the architecture/nature of Email and resources required to perform the restoration. Therefore, DTS will:

- only restore individual mailboxes from specific Exchange backup tapes for legal matters upon request from the County Attorney's office.
- only restore individual mailboxes from specific Exchange backup tapes for public information act requests upon concurrence from the County Attorney's office and payment for costs incurred from party seeking information.
- only restore individual mailboxes from specific Exchange backup tapes for other purposes upon request approved by the user's Department head and CIO.
- undelete mailboxes within 10 days of deletion upon request. Mailboxes deleted for more than 10 days require Exchange backup tape restoration, see above.

3.7 Enterprise Hosting Infrastructure Platform

Principles

The Enterprise Hosting Infrastructure (EHI) is the framework the County uses to deploy its enterprise applications. The County's EHI goals are to integrate business processes across the County by integrating and extending existing web applications. The County benefits from EHI because it promotes enterprise-wide data standardization, reuse, interoperability, and information management across applications and agencies. Reducing cost and development time, EHI facilitates common solutions for business processes, lower operational costs, increased business productivity, and better utilization of resources.

EHI encompasses most components of the County's IT Framework: Enterprise and Web Application Domains (see Montgomery County Government Enterprise Architecture Application Architecture), Software as a Service (see section 3.21), Deployment Domain (see section 3.4), Network Domain (see section 3.12), Security Domain (see section 3.3), Reporting Domain (see section 3.15), Geographic Information Systems Domain (see section 3.8), Help Desk (see section 3.9), Active Directory & Single Sign On (see section 3.1), Email System Services (see section 3.6), Service Enabled Domain (see section 3.16), Enterprise Server Management (see section 3.20), Database Hosting Infrastructure (see section 3.22) and System Operations Domain (see section 3.17). Figure 3-3 demonstrates the components that make up the County's EHI.

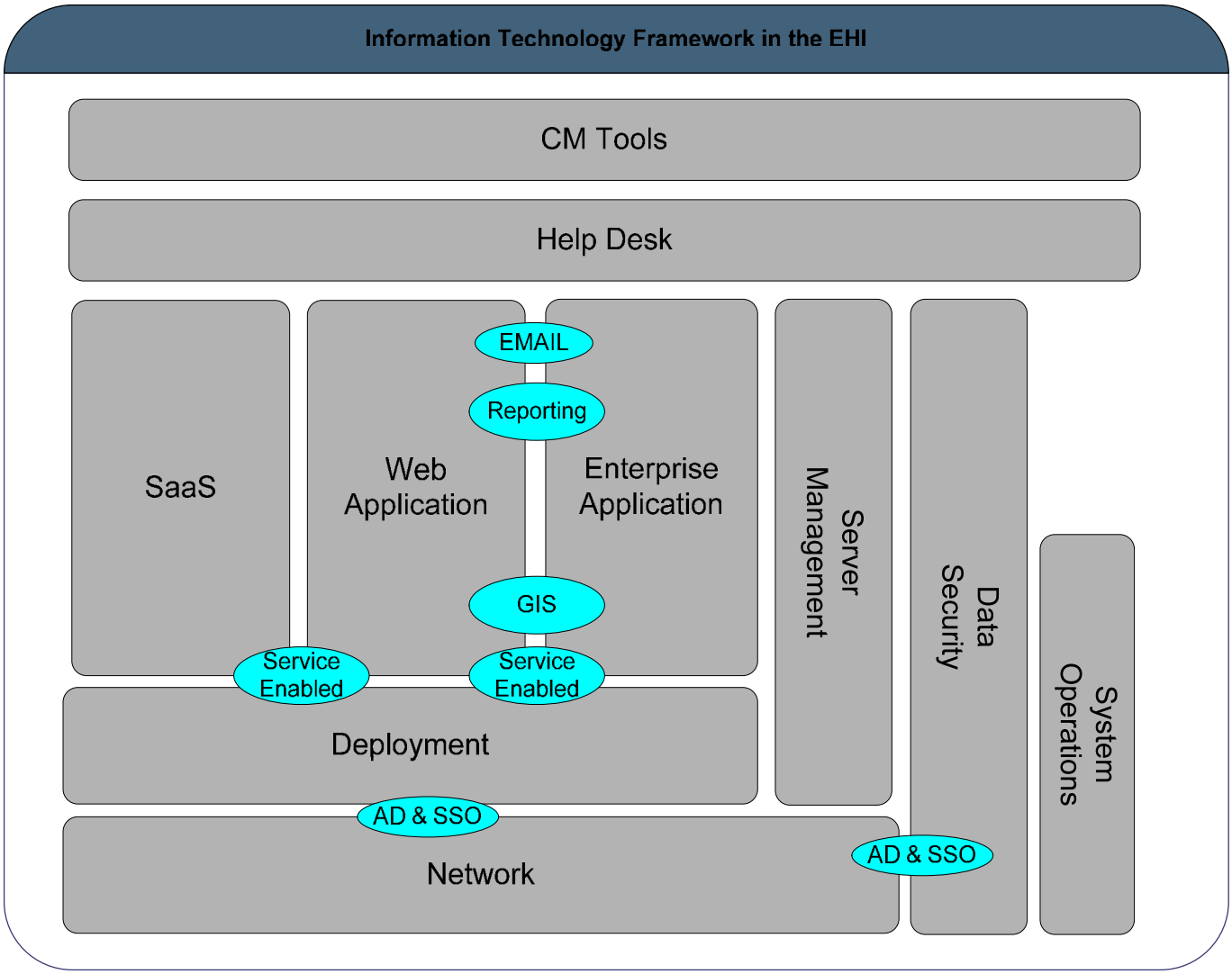


Figure 3-3 Enterprise Hosting Infrastructure Components

When a new application is targeted to be hosted in the EHI an intake form is filled out for the application. The intake form contains information about the application with one aspect of the information being the NIST Confidentiality, Integrity and Availability requirements for the application.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Server Team
- DTS Enterprise Services Architect

Components

Architecture Overview

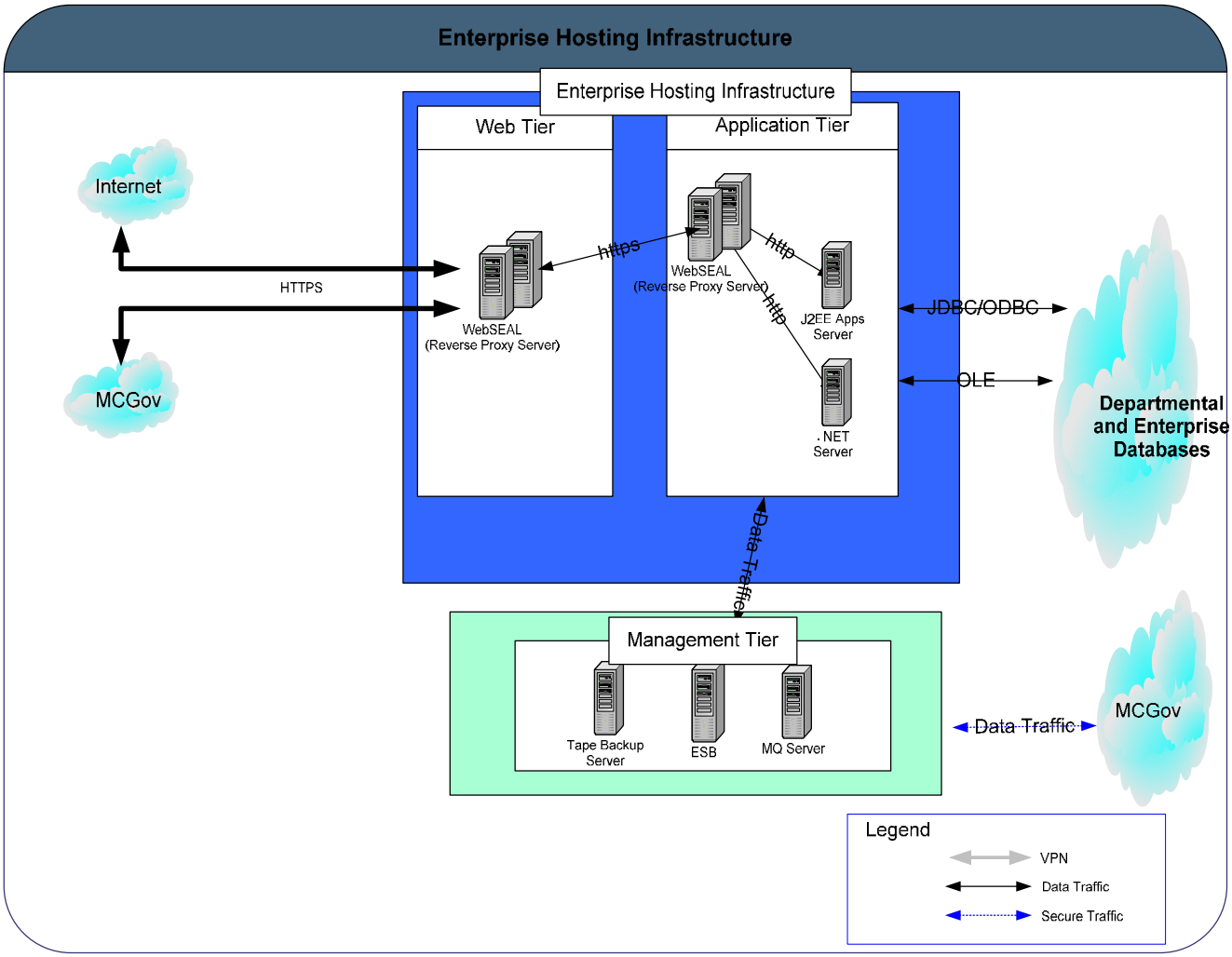
In general, the EHI architecture is based on three layers of application deployment:

- the first layer incorporates security and Single Sign On (SSO) components for the application
- the second layer incorporates the presentation and business logic of the application
- the third layer incorporates the data model of the application

Only the first layer is located in the Web Tier. The Web Tier serves as the gatekeeper for client access to Web Applications that serve Internal County Users as defined in Active Directory.

The second layer is located in the Application Tier. It is the location for the Application Servers.

The third tier is the database tier and is supported through individual departmental database servers as well as Enterprise Database Servers hosted in the Database Hosting Infrastructure (see section 3.22). All traffic between the Web tier to the Application Tier is encrypted with certificate Secure Socket Layer (SSL). All Web traffic (from the internet and the intranet) designated to the application server in the Application Tier will be routed thru the Web Tier. The following paragraphs describe the components that make up the platform architecture.



Active Directory

Microsoft Active Directory is the master user registry for all county employees and for all applications hosted in the EHI (see section 3.1 – Active Directory (AD) and Single Sign On (SSO) Services). All LDAP traffic from the Web and Application tiers is encrypted (LDAPS) and accesses one of the Active Directory controllers. Active Directory also provides the primary DNS service for the Application tier of servers.

Tivoli Access Manager (WebSEAL)

The County has set up Tivoli Access Manager (TAM) to maintain a directory of user roles that have permission to access specific applications. TAM uses Active Directory as the master for user and user group objects and extends the Active Directory schema to add more attributes to the user class. TAM is automatically synchronized with Active Directory and provides an extra layer of security. It intercepts all application access by a user and ensures that they are properly authenticated. In addition, it allows users to sign on one time and access multiple applications. TAM checks against Active Directory one time to confirm or "validate" an individual's roles or permissions to application(s). This function is known as Single Sign On (SSO) (see section 3.1 – Active Directory (AD) and Single Sign On (SSO) Services).

Application Server

JBOSS is used to serve the County's J2EE applications. All JBOSS servers are located inside the Application tier. Microsoft.Net servers are also hosted inside the application tier to support county .Net and ASP applications. The WebSEAL server in the Application tier directly accesses the HTTP services of the Application servers. Beside the standard J2EE and .Net applications, other commercial off-the-shelf COTS applications are hosted in the Application Tier, for which the WebSEAL provides the SSO integration.

Enterprise Service Bus (ESB)

The Enterprise Service Bus (see section 3.16 – Service Enabled Domain) provides secure methods of transferring data between different platforms across different Tiers. It uses the following methods of data transfer:

- IBM MQ
- SFTP
- FTP (PGP encrypted)
- Webservices
- Secure Mail (S/MIME)

Servers located in the EHI Application tier can use the ESB to securely interface with servers outside the EHI platform.

The ESB is also used for secure file transfers into and out of the county.

Database Server

The database servers are located outside the EHI as either Departmental Database Servers or as Enterprise Database Servers that are hosted in the Database Hosting Infrastructure (see section 3.22). The county supports both Oracle and Microsoft SQL servers under the DHI architecture. Application servers can access the database servers directly thru JDBC/ODBC/OLE.

Platform Choice

Hardware

All servers are Intel based and manufactured by Dell Computers. The hardware sizing is based on the County standard as outlined in the Deployment domain (see section 3.4 – Deployment Domain).

Operating System

Virtual Machine technology is used in the platform architecture. Server virtualization increases the efficiency and effectiveness of deploying and developing new technology. It aides server consolidation and capacity optimization by utilizing excess hardware capacity. The ease of cloning of the entire virtual system provides easy backup and restore capability. This is an important operational practice for the high performance and high availability of applications within the EHI.

The Operating Systems supported on the servers are:

- CentOS
- Microsoft Windows Server

CentOS is an Open Source OS which uses the Red Hat Linux kernel and hence is an “identical twin” of Red Hat Linux.

Services

Time Service

Time services are supplied through two time servers. Windows machines are synchronized through the Active Directory Domain controllers. UNIX machines are synchronized through the county UNIX time server.

Backup Service

The EHI uses the backup services of the System Operations Domain. Once a week each VM Guest has a snapshot taken of its image. That image is then backed up through System Operations Domain services.

Refer to the System Operations Domain (see section 3.17) Server Backup and Recovery Section for details on retention and backup times.

Antivirus Service

Antivirus service is provided on the Windows Machines. Virus signatures are automatically synchronized from the county central Antivirus server.

SMTP Service

Email services are provided through access to one of the County Exchange Servers (see section 3.6 - Email System Services).

Storage Service

Storage is provided through large local hard drives on each server

Directory and User Registry (LDAP Server) Services

Directory and User Registry services are supported through Active Directory. For LDAP, only the LDAPS protocol is supported.

Certificate Server

Certificate services are provided through a Microsoft Windows Certificate Server and issues certificates based on the MCGOV root certificate.

Network

The EHI uses the Network Domain's Firewalls and Switches (see section 3.12 - Network Domain).

The EHI is separated from both the Intranet and the Internet through one or more stateful firewalls. In addition, firewalls are also used to separate tiers internally within the EHI.

Security

Tivoli Access Manager (TAM)

A set of WebSEAL reverse proxy servers are located inside the web and application tiers to receive encrypted traffic (SSL) from the intranet and the internet. The WebSEAL server within the Web tier will authenticate the user with the LDAP server in an encrypted form (LDAPS). In turn, it will pass the traffic to a WebSEAL server (identified by the part of the web URL called junction) inside the Application tier thru an SSL channel. The WebSEAL server inside the Application tier passes the traffic in non-SSL fashion to the application server to process. The application server then returns the response data back to the Web tier WebSEAL server through the same SSL channel.

The WebSEAL to WebSEAL junction optimizes the traffic inside the Application tier while providing security to the Application tier. All Tivoli web servers, including the policy server, Web portal manager, and TAM application server are located inside the application tier.

Application Principles

The general principles that an application must follow are:

- Access to the Application's Application Server must pass through the Web Tier and the Tivoli WebSEAL Servers
- Client access is via HTTPS only
- Access can be from the Internet or MCGov Intranet
- The ESB is used for non-client inbound and outbound traffic between the EHI and the MCGov Intranet with all traffic being point to point
- inactive session timeout
- Firewall is a stateful firewall
- Application access must be through the stateful sessions maintained by Tivoli

Standards

EHI Hosting Agreement

A requesting team or department must read and agree to the EHI Hosting Agreement. The EHI Hosting agreement lists roles and responsibilities for the service.

Administration Policies

- No access to resources other than by DTS employees performing administration services
- Monthly patching of Operating System and middleware software
- Virus updates every 10 minutes
- Weekly VM Guest backups
- Active Directory Group Policies (DTS Server Team Administrators are the only persons allowed to administer the machine and processes)
- Quarterly review of the Firewall Rules
- Quarterly review by Stakeholders of their application intake information
- Outage reports through HelpIT updates
- Maintenance window announcements through HelpIT updates
- Each ESB integration has its requirements documented, implementation documented and data transfers audit logged.
- Each Application has a standard Help Desk Incident Script. Custom scripts can be created based on the Applications need.
- Each Application must use Active Directory Authentication
- Highly Recommended that each application use Active Directory Authorization

Application Hosting Service Intake Form

A requesting team or department must fill out an Application Hosting Service Request Form. The form contains:

- Application Name
- Application Description
- NIST Security Classification for Confidentiality, Integrity, Availability (High, medium, low)
- Owning Department(s)
- Department(s) Administrators contact name
- Department(s) Administrators contact email
- Department(s) Administrators contact phone
- Department(s) Administrator Active Directory account
- Type of Package (J2EE, .Net)
- Package Contents
- Database(s) accessed
- Incident Response Plan
- Configuration Plan
- Is the Application Internet Facing?
- Is the Application going to use Active Directory Authorization? (If so, please list the AD groups)
- Expected lifetime of the application

Application Policies

The following are standards and guidelines the County has set forth for its EHI Applications.

- Performance Guideline – The County expects a turnaround time for Enterprise Applications in 3 seconds or less
- Availability Guideline – The County expects an Enterprise Application be available no less than 99.5% of the time.
- ADA compliant – The County expects an Enterprise Application to be ADA compliant.

- HIPAA compliant – The County expects an Enterprise Application that handles HIPAA covered data to comply with the HIPAA Privacy Rule and the HIPAA Security Rule.
- Each Application will use Active Directory Authentication. Applications are strongly recommended to use Active Directory Authorization. Applications are provided with one or more Application Groups to manage Authentication. J2EE applications are provided with a library that validates authentication against the groups. .Net applications are provided with a similar design pattern.
- Application Security Standards – See Appendix C
- Coding Standards – See Appendix D
- Technical Design Template
- The County has standards for Java files to have the following package structure:

  gov.montgomerycountymd.<<dept>>.<<application>>.<<module>>

  where

  dept will be the short name of the department that owns the application
  application will be the short name of the application itself
  module will be the implementation section

- The County has standards for .NET namespace:

  gov.montgomerycountymd.<<dept>>.<<application>>.<<module>>

  where

  dept will be the short name of the department that owns the application
  application will be the short name of the application itself
  module will be the implementation section.

Quality of Service

- Multiple deployment environments have been set up for application deployment and testing:

  Development – WebSeal junctions are directed to a developer(s) machine

  Test/Staging – A separate physical environment for Test and Staging

  Production – A separate physical environment for Production

- Automatic Sync Up of TAM with Active Directory every day, so employees' records inside Active Directory are synchronized with TAM.

- Enhanced TAM passes user attributes in Active Directory to minimize the general LDAP access from application to Active Directory.

- There is an ACL (Access Control) rule defined for Production TAM in such a way that test Active Directory accounts can NOT access the Production applications.

- The Active Directory Application Authorization Model allows the delegation of application administration to different application administrators in the County.

- Heart Beat uses same SSO access paths to SSO application to provide continual monitoring.

- Using VM and Microsoft disk mirroring, servers in EHI can be easily restored and tested with updates or patches.

- WebSEAL provide standard SSL protection (FIPS 140-2 certified) for the County's existing applications.

Physical Security

The networking switches and firewalls as well as the hosts that support the Production EHI are all located within one of the Department of Technology Services Data Centers (see section 3.17 – Systems Operation Domain).

Help Desk Support

A key component of the EHI is the Help Desk (see section 3.9 – Help Desk Services). It provides a single point of contact for the users of applications hosted within the EHI. The Help Desk resolves problems or, as needed, routes problems to the EHI administrators.

As part of the intake process for a new EHI application a support plan is developed with the help desk. The support plan includes information such as:

- Identifying the business system owner
- Identifying the EHI Administrator contacts
- Identifying common problems and their resolution that a level 1 support person can handle
- Identifying the contact for level 2 problems

Server Administration

Administration of the EHI Servers is performed by the DTS Server Team (section 3.20 – Enterprise Server Management)

Deployment Model

A J2EE application must be packaged into an EAR (Enterprise Archive) file for deployment. Even if the application contains only the Web components (a collection of Web Archive WAR) files), it should be packaged into an EAR file.

Applications may not package the libraries' JARs for the County's standard components, such as Oracle, LDAP, and WebSphere. The County should have full flexibility to deploy upgrades for its standard libraries without altering the applications.

Every J2EE Web component should be self-contained. All the required libraries should reside within the WAR package. Similarly, every other component (such as EJBs) should be self-contained within EAR package.

Every application may accompany a folder with subfolders for configs, scripts, and properties files.

Every application package must accompany a Configuration document. This document should clearly

explain the prerequisites and steps for installing the application. The document must include:

- List of files in the package
- List of configuration options and description of each
- List and description of 3rd party dependencies
- List of log files, their location, and description

The County encourages programmers and analysts to include a troubleshooting section in their Installation and Configuration documents to help avoid known mistakes. The County also encourages programmers and analysts to include a health-check section to check the health of the application after installation or after a restart.

The County encourages applications to write log error condition messages in the standard format. The document may indicate the format and the expected error messages. All applications shall support multiple log levels which can be modified without re-starting.

3.8 Geographic Information Systems Domain

Principles

The County has designed and implemented a Geographic Information System (GIS) to deliver geospatial data to spatially enabled desktops, Web-based applications, and location services. The system generates both soft and hard copy and Web-based cartographic/mapping presentations enabling data analysis and decision support services. The County has dedicated resources to create, maintain, manage, and store geo-spatial data.

The County has two definitions of spatially enabled services. One is a service capable of integrating spatial data with other business data across multiple, heterogeneous data sources. The other is a service supporting abstract data types (images, text, and spatial data) spatial operators, functions, and spatial locator indexes. The County implements Environmental Systems Research Institute's (ESRI) GIS data models and ArcGIS suite of software.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS GIS Team.

Components

The GIS configuration is designed to be flexible, fast, scalable, reliable, manageable, and secure in order to satisfy the needs of a wide variety of users and customers. Casual users typically use GIS services delivered by Web and desktop applications to perform basic tasks such as generating maps and travel directions or finding a map feature such as a place of interest. Intermediate users perform basic mapping functions in addition to inputting data and performing basic geo-spatial analysis (queries, geo-coding, buffering, overlay, etc.). Casual and intermediate users use Web browsers to access customized *ArcIMS* or *ArcGIS* Server map and image services/viewers, as well as ArcView, ArcReader, or ArcExplorer (free viewer) software products. Advanced users use GIS and cartographic software products such as ArcGIS (one of the three tiers), ArcSDE/Oracle, ArcView , and Adobe Illustrator and Photoshop (used for mapping) to produce, maintain, manage, analyze, and map geo-spatial data sets. Advanced users also use GIS software products to create customized applications on both the desktop (Arc Macro Language, Avenue, Visual Basic, and Visual Basic for Applications) and the Web (Active Server Pages, XML, HTML, JavaScript, and Perl). Recent experiments with GoogleMaps has also shown great potential for presenting County's geo-spatial data in a vivid way.

System requirements (provided by ESRI), and customer requirements dictate the County's GIS design. Figure 3-5 and Table 3-6 provide an overview of the GIS system and Web architectural designs.

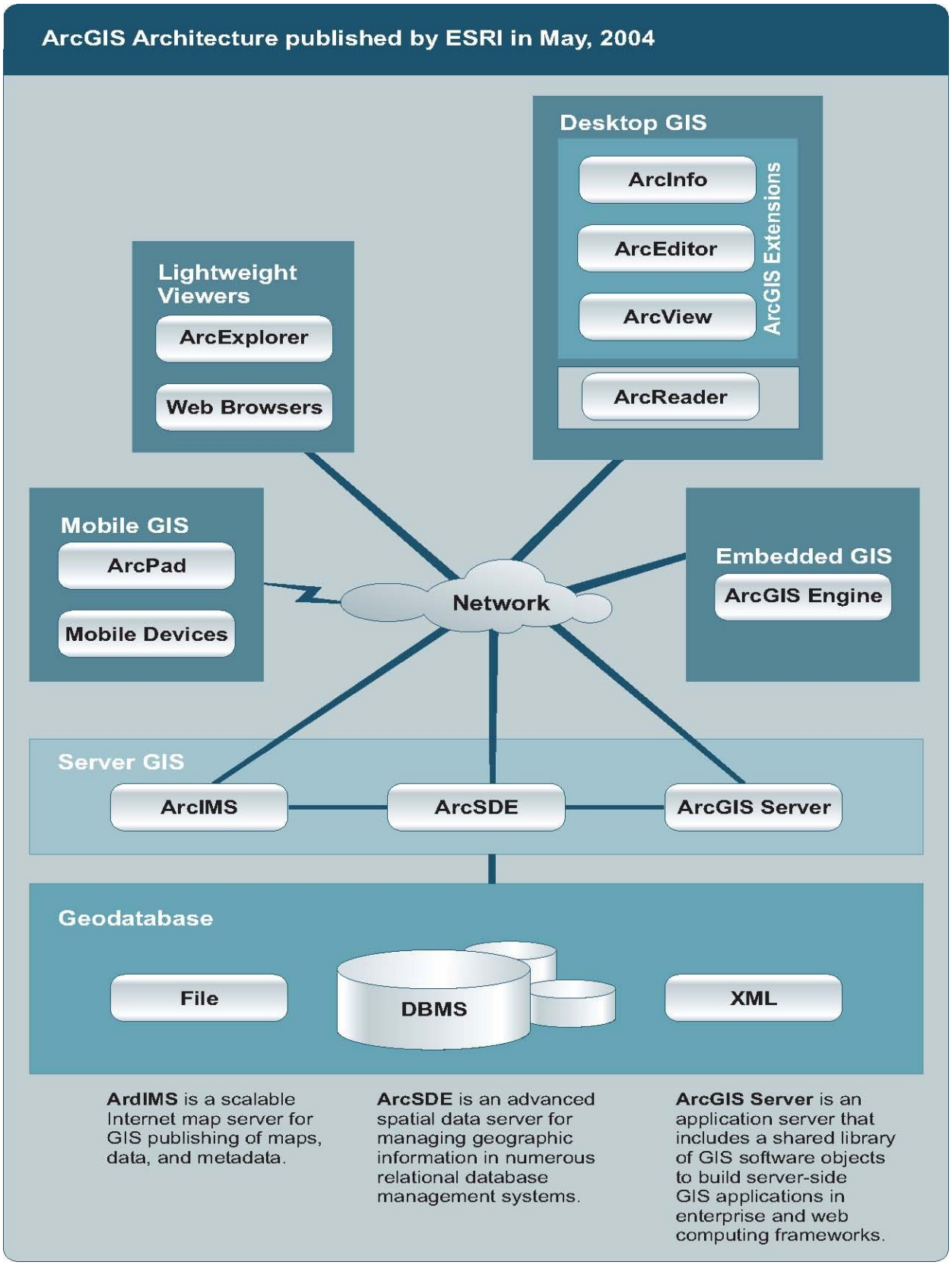


Figure 3-5 ArcGIS Architecture [1]

[1] ArcGIS Architecture, Published by ESRI, May 2004

Table 3-6 below identifies the GIS software that has been installed in the County. These versions of ArcGIS software, ArcSDE middleware, and Oracle 9i or 10g database have helped to centralize the GIS data layers to the new ArcGIS Geo-data model.

GIS Software Components		
New Version		**Platform**
Enterprise GIS	Server-side Geo-processing environment - ArcGIS Engine: with embeddable GIS components ("Maps for Apps")	Intel PC MS Windows
ArcGIS Tiers	ArcInfo ArcEditor ArcView ArcReader (free)	Intel PC MS Windows
ArcGIS Extensions	ArcGIS Business Analyst (at DED) ArcGIS Spatial Analyst ArcGIS 3D Analyst ArcGIS Geostatistical Analyst ArcGIS Survey Analyst ArcGIS Tracking Analyst ArcGIS Publisher ArcGIS StreetMap ArcGIS Schematics ArcScan for ArcGIS ArcPress for ArcGIS MrSID Encoder for ArcGIS	
Free ArcGIS Add-Ons	Tablet PC Support for ArcGIS ArcMap GPS Support Districting for ArcGIS	
Mobile GIS	ArcPAD ArcPAD Developer Tool Kit	Pocket PC Windows CE
Database	ArcSDE – middleware Oracle (licensed separately from Oracle Corp.)	Oracle
Web GIS	ArcIMS - RouteServer ArcGIS Server ArcExplorer (free)	Wintel Server

Table 3-6 GIS Software Components

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
ArcGIS software – core modules
ArcGIS Extensions
Geo-database data model, ArcSDE and Oracle
ArcIMS, ArcExplorer, and ArcGIS Server
Visual Basic for Applications
Develop Geo-processing Scripts Using Python
Utilizing ArcObjects for application development
XML, ASP
J2EE, JavaScript

Standards and Guidelines

GIS Servers

- Administrator privileges are limited to DTS employees performing administration services
- Monthly patching of GIS Servers Operating System and middleware software
- Virus signature updates every 10 minutes
- Read only access provided to other departments to use ArcGIS
- DTS backs up Enterprise GIS Servers for disaster recovery purposes. DTS' current recovery process is to restore servers in the event of system crashes, facility loss, or some other disaster. To support the current model, the GIS Domain uses the backup services of the System Operations Domain (see section 3.17 System Operation Domain). Refer to that domain for backup retention times.

GIS Data

- Some departments maintain their own department specific GIS maps and data layers but send their data to the DTS GIS team to keep in the County Central Repository
- Street Addressing standard
- Centerlines, districts, buildings, and places of interest maintenance procedures
- Secure Web application requests and approval forms
- GIS data requests form

- All County employees having access to the Enterprise computing resource can access all commonly available GIS data layers.
- County GIS data, hardware, and software are for business use only.
- DTS' GIS coordinates the distribution of the County's GIS data to outside entities. Consultants performing contracted County projects can be supplied needed GIS data free of charge. This data is sold to outside entities and transferred electronically or by CD/DVD media.

3.9 Help Desk Services

Principles

The IT Help Desk provides a single point-of-contact, centralized support to County employees and contractors using the County's IT Infrastructure. The IT Help Desk resolves problems or, as needed, routes problems to other support organizations to assure that they are resolved properly.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Client Computers (DCM) Team.

Components

The County uses Service Desk Express (SDE), a customizable, browser-based service management system from BMC Software, to manage problem identification, analysis and resolution. This software was designed specifically for the mid-sized business and provides enough functions for the County's centralized IT Help Desk. As it is currently implemented, Service Desk Express is used by the County for service management, asset management, self-service ticketing, and reporting.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Service Desk Express
Customer Service
Problem Analysis & Resolution
MS Office Products
MS Windows OS/Platform
Networking

Standards and Guidelines

Level 1 Support - The IT Help Desk will provide support for all IT requests it receives by attempting to resolve the problem immediately over the telephone. Level 1 includes support for standard desktop PC

hardware, software, and operating systems. The IT Help Desk shall support new, standard software whenever adopted by the County. The IT Help Desk shall also be available for support and service requests received via e-mail and self-service requests created in the Self-Help Information Portal (SHIP).

The responsibilities of Level 1 Analysts are to receive trouble calls, enter the calls into Magic Service Desk, document the problem, and perform remote troubleshooting. If the problem does not pertain to the desktop PC environment (e.g., mainframe issue) the call will be transferred to the appropriate support organization within the County's IT Help Desk. The Level 1 Analyst coordinates the problem resolution process with other IT support resources, and communicates the status of the problem to the end-user. To ensure user satisfaction, the Service Desk Express system will automatically notify the client via email when the problem has been resolved.

When it is unable to resolve a trouble report remotely, Level 1 will escalate the resolution process to Level 2. Level 2 personnel will inform Level 1 personnel of the status of the problem and the actions being taken to resolve it. The responsibility to coordinate problem resolution, and to document the status of problems, remains with Level 1. This is facilitated by the communication capabilities of the Magic Service Desk.

Level 2 Support - If the call cannot be resolved by Level 1 support, the request will escalate to Level 2 Support, which provides Senior IT Help Desk Analysts, Hardware Technicians and Maintenance Technicians. The IT Help Desk will dispatch technicians, as needed, to provide desk-side assistance. Upon escalation to a Level 2 request, the IT Help Desk shall immediately assign an appropriate technician. This technician will call the user to acknowledge receipt of the request, analyze the problem and attempt to initiate resolution over the telephone. Level 2 support personnel shall have advanced skills on the standard County's PC hardware and software. Should further support be required, the call will then be transferred to other support organizations in the County's IT Help Desk.

Problem Escalation - If the problem has not been solved by Level 1 or Level 2 support, it will escalate to the IT Help Desk Support Manager for resolution. Unresolved issues will escalate to the Desktop Computer Modernization (DCM) Program Office. The IT Help Desk generates monthly trend analysis reports. These trend analysis reports help to identify repeat problems, which might indicate systemic issues beyond the scope of the problem reported.

Service Levels - Service level indicators for the IT Help Desk are established in the DCM Contract and are used to show performance level. The service level indicators established are the Minimum Acceptable Level (required) and the Incentive Level (incentive goals).

Phone Number

Help desk phone number is 240-777-2828.

3.10 Interactive Voice Response Domain

Principles

The Department of Technology Services' goal is to develop IVR strategies that improve customer service and lower operational cost by integrating all County IVR functions into one enterprise platform. The current platform will expand to accommodate a variety of applications, reduce application redundancy, and service the County in a more efficient way.

Interactive Voice Response (IVR) is a technology that enables callers to obtain information stored in a corporate database. IVR technology uses the familiar telephone keypad as an information retrieval and data gathering conduit. Recorded voice messages prompt and respond to caller inquiries and commands.

IVR's functions range from the simple process of selecting options stored in a computer (such as the single digit menus deployed throughout the County), to more complex interactive exchanges that rely on database lookups, such as the Finance Department's tax line script, and Health and Human Services' payment status system.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS PBX Telephone Services Team.

Components

The Avaya IVR server provides call processing and media services, as well as standard operations, administration, and maintenance. Working with existing Web infrastructure, the system uses HTTP, XML, Java, and VoiceXML languages. At the heart of the IVR is a UNIX server, which provides high port density and uptime reliability. IVR uses a distributed client/server Natural Languages Speech Recognition architecture to meet the County's customer needs successfully, in a cost-effective manner.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
SQL programming and DBA
Java API, C++ Programming
Vonetix Software Programming
XML, VoiceXML

Standards and Guidelines

Functions

An Interactive Voice Response system must be able to provide the following functions:

- Call answering and routing: the IVR system will answer a call. Callers then select a menu item to direct their own call.
- Information retrieval from a database via telephone or internet via Web interface: the caller accesses database records using telephone keypad or a Web site.
- Touch-tone and voice data input: the caller uses DTMF keypad tones or “natural” voice speech for inputting data.
- Text-to-speech capabilities: the system artificially generates spoken words from textual information.
- Voice recognition: the system identifies a particular person’s voice.
- Speech recognition: the IVR system must have the ability to understand human “natural” speech.
- Fax back confirmation and information fulfillment: callers can request and receive information and confirmation by fax requested documents, 24hours per day, for 7 days per week.
- Voice forms for short voice messages: callers can verbally respond to recorded questions. The answers are stored for later transcription.

Enterprise IVR System	
Scalable	• Upgradeable • Scalable by ports (analog, digital, ISDN) • Capacity to increase memory • Ability to add disks
Administration	• Managed by internal staff or outsourced. • Determined by "cost management" • Secured access • User friendly administration - GUI click and drag • Easily modifiable script changes • Procedures for change management, testing, and problem resolution
Interoperability	• Provide access and control to multiple host, databases, networks, and telephony interfaces • Integrates with telephony, data and information systems • Website integration
Maintenance	• 24x7 vendor maintenance availability • One contact and local service support • Written and approved service level agreement • Reliable 99.9% uptime (critical system) • American Disabilities Act (ADA) Compliance.
System hardware and software	• Application may or may not reside on the system • Multi-tier voice and data integration CTI, TCP/IP, call center. • Accepts multiple IP addresses • Voice module text to speech, speech to text, multiple languages, both 'natural" speech and key work speech, TDD-TTY compatible • Capable of more than one application on a "box" administered separately. Each application can be taken down for maintenance and upgrade without affecting other applications
Redundancy/Disaster Recovery	• Hot swappable parts • Disaster recovery features • Capability for on-line back-ups • Redundancy in case of hot site catastrophe • Business continuity considerations • Dual power supply • Minimal single point of failure

Table 3-7 Enterprise IVR System

3.11 Mainframe Application Services (deprecated)

Principles

Montgomery County Government owns and operates an IBM mainframe to support the County's legacy applications, which are General Ledger, Criminal Justice, Payroll, Purchasing, Fixed Assets, Budget and Tax Assessment.

The mainframe is an IBM Z9 BC Type-Model 2096-R07 B03 three processor 109 MIPS machine with one Crypto Express2 and one DB2 zIIP sub processor. It is running the z/OS v1.9 Operating System.

System software supported on the mainframe includes:

- CA-7 job scheduler
- CA-1 tape management system
- CA-Opera automated systems manager
- CA-Librarian source code management
- DB2
- CICS TS
- IMS DB/DC 8
- SAS statistical analysis system
- EOS report archive and distribution

The County is in the process of retiring the mainframe and all applications running on it. Initial retirement plans have been developed for each of the applications with the mainframe having a target retirement date of 1st quarter 2013.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Operations Management Support Team
- DTS Enterprise Systems Team

Components

Application services on the mainframe include:

Payroll and Personnel - Integral's Human Resources Management System (HRMS) v9.5 is a Payroll and Personnel application implemented using COBOL, CICS and DB2. **(Functionality migrated to the County ERP project – January 2011)**

Position Control System (PCS) - PCS is a SAS/AF application with a DB2 database. **(Functionality**

migrated to the County ERP project – January 2011)

FAMIS - FAMIS v 4.2 is the General Ledger accounting system. It is a KPMG product developed using COBOL and CICS, and adapted for DB2 by BearingPoint consultants. **(Functionality migrated to the County ERP project – July 2010)**

ADPICS - ADPICS v4.5 is the Purchasing system. It is a KPMG product developed using COBOL and CICS, and adapted for DB2 by BearingPoint consultants. **(Functionality migrated to the County ERP project – July 2010)**

FAACS - FAACS v4.2 is the Fixed Asset accounting system. It is a BearingPoint product using COBOL, CICS and DB2. **(Functionality migrated to the County ERP project – July 2010)**

BPREP - BPREP v4.2 is the Budgeting system. It is a KPMG product developed using COBOL, and CICS, adapted for DB2 by BearingPoint consultants. It is an online, real-time environment with a batch interface to FAMIS.

Tax Assessment - Tax Assessment is an in-house developed application using COBOL, IMS/DC, and IMS/DB. To produce Property Tax Bills, it conditions the property assessment data from the State of Maryland, for submission to the MUNIS system.

EOS - Enterprise Output Solution (EOS) is the Report Archive and Distribution system from Rogers Systems Development (RSD). It stores and distributes reports from all of the mainframe applications. Reports are available for viewing through VTAM. Security is at the page level. There are over 600 users defined to EOS and tens of thousands of stored reports available for viewing or redistribution.

Criminal Justice Information System (CJIS) – CJIS was the principle source of offender processing information, including criminal history information for over 20 years. The County's IJIS program has been replacing components of the functionality over the last several years with the final functionality anticipated to be replaced January, 2013.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
COBOL
CICS
DB2
IMS
SAS
JCL
Crystal Reports
FTP/SFTP
SQL

Standards and Guidelines

The mainframe is available 24 hours per day, for 7 days per week, except for the regularly scheduled Initial Program Load (IPL) on Sunday mornings between 8 AM and 12 PM. When needed, Mondays and Wednesdays from 6 PM to 8 PM are reserved for system maintenance/update outages.

Online data entry to the mainframe applications is available through CICS and IMS/DC from 7 AM to 6 PM each business day. DB2 databases are up for 23 hours a day. They are unavailable from 4 AM to 5 AM each business day because this time is reserved for SNAP backups. IMS databases are unavailable from 6:15 PM to 7:00 PM, and from 4 AM to 5 AM each business day because of backups.

3.12 Network Domain

Principles

The County is unique among its peers because it is its own telecommunications carrier. The County has undertaken several major initiatives to isolate itself from the uncertainty and expense of purchasing telecommunications services from the incumbent local exchange carrier (ILEC). Two major initiatives are the construction of a private facilities based electro-optical network (FiberNet I) and the installation of a large private branch exchange (PBX). These two initiatives have been complemented by two follow-on projects that leverage these investments. The first of these new initiatives was the installation of a metro-Ethernet network in 2007. This network is referred to as FiberNet II. The second initiative is the deployment of Voice over Internet Protocol (VoIP) as an alternative to digital wireline dial tone. These projects are well under way and very successful.

FiberNet is the name of the County's network. Based on economics and public safety concerns, the County can choose between FiberNet and the Local Exchange Carrier for telecommunications services and solutions. Telephony, public safety radio, data, secure Internet access, and video application services ride over FiberNet. From the County's perspective, FiberNet is a self-owned and operated electro-optical wide, campus, and local area network infrastructure, supplemented, when necessary, with ILEC frame-relay and TDM services.

The County built and manages its own network infrastructure. FiberNet is a robust and resilient service provider class network composed of over 500 miles of optical fiber plant, ATM and Ethernet switches, routers, one and ten Gigabit Ethernet (GbE) links and frame-relay circuits. These technologies are combined to deliver connectivity solutions that are efficient, bandwidth-rich, and economically justifiable. The first principles of engineering design are performance, security, reliability and availability, and these principles dominate FiberNet's daily operation. Cost recognition, reduction and containment are the economic principles that guide the operation of the network. FiberNet is monitored and evaluated against these principles and improved accordingly.

Montgomery County's network infrastructure supports a distributed user community, providing public safety and health services, traffic signal management, highly successful Internet-based eGovernment, back-office business applications, justice information systems and education.

FiberNet is a multi-agency telecommunications resource that is subject to inter-agency governance. FiberNet's strategic planning, budgeting and operational oversight is a matter of concern and involvement by the County Council which created the Information Technology Planning and Coordinating Committee (ITPCC) and its subgroups. This governance structure manages the direction of FiberNet, approves budgets and oversees the stewardship of DTS in operating the network.

FiberNet is a multi-service network infrastructure supporting voice, video and data to hundreds of sites within Montgomery County. The network has been operational for over eight years. New sites are added regularly.

FiberNet is currently undergoing an upgrade to a next-generation metropolitan area network technology based network called FiberNet II.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the Network Services Team.

Components

FiberNet is a standard-based infrastructure implementing IETF, IEEE and ITU-T protocols on hardware and software products from Cisco, GDC Communications, 3Com Networks, VBRICK and other major equipment manufacturers. Standards implemented within the County's network infrastructure are shown in Table 3.12. Element managers and network management system tools (NMS) help maintain control of the network by tracking utilization, reporting faults, and maintaining configurations. NMS products currently in use or planned to be used are Cisco Works, GDC ProSphere V4, IBM Netcool, Statseeker, and HP/Open View Network Node Manager.

FiberNet I

FiberNet I is a multi-service network infrastructure supporting voice, video and data.

Major components include a County owned and operated fiber optic plant, ATM and Ethernet switches, ATM integrated access devices, multi-protocol routers, firewalls, video codecs, wireless access points, and bridges, as well as element managers and network management systems. Table 3.12 lists protocols and standards supported by the County network.

The County employs three major technologies in its wide area network (WAN). These are electro-optics over the County's fiber optic plant, 802.11 wireless bridges, and Verizon's frame-relay. FiberNet I employs an electro-optical core network using ATM, Fast Ethernet, and one and ten Gigabit Ethernet (GbE) technologies to deliver connectivity to many County locations. FiberNet is a partially-meshed network topology, connecting eleven major hub sites spread throughout the County. County offices, fire houses, police stations, and schools having hub locations receive OC-3 ATM or Ethernet hand-offs to the appropriate edge device. Additionally, County locations within the Rockville core area may be directly attached to FiberNet using GbE optical links. Over 110 County locations are connected using Verizon's Frame-Relay services. Where "fibering" costs are high, or the facility is leased, wireless 802.11 bridging is used to connect sites to FiberNet I.

Local Area and Campus Area Networking uses three physical media and three link layer protocols. Physical media include copper (cat 5e & 6), multi-mode fiber and air-interface (wireless). Increasingly, wireless is becoming more important and more prevalent throughout the County. Link layer protocols include 10BaseT, Fast Ethernet, GbE, and 802.11 a/b/g. At the network layer, the County only supports routing the Internet Protocol (IP).

FiberNet II

Montgomery County determined that FiberNet should adopt a service provider network model for the next generation of FiberNet. Service providers like AT&T and Verizon have moved from ATM and frame-relay technologies to metro-Ethernet and Multi Protocol Label Switching (MPLS). In doing so, they have been able to offer virtual private network (VPN) solutions based on logical network separation at the IP layer. A major advantage of this combination of technologies is the easy segmentation of networks so that departmental isolation is based on security requirements and business needs. For Montgomery County Government, key workgroups and departments will be given their own virtual private network with

common and shared services being accessed via a stateful firewall. The service provider model enhances FiberNet's ability to provide secure network services to critical Public Safety and Health departments in the county government. It is designed to better respond to Compliance Initiatives as well as improve survivability from network attacks.

Figure 3.8 depicts the general design of FiberNet II.

FiberNet II Core

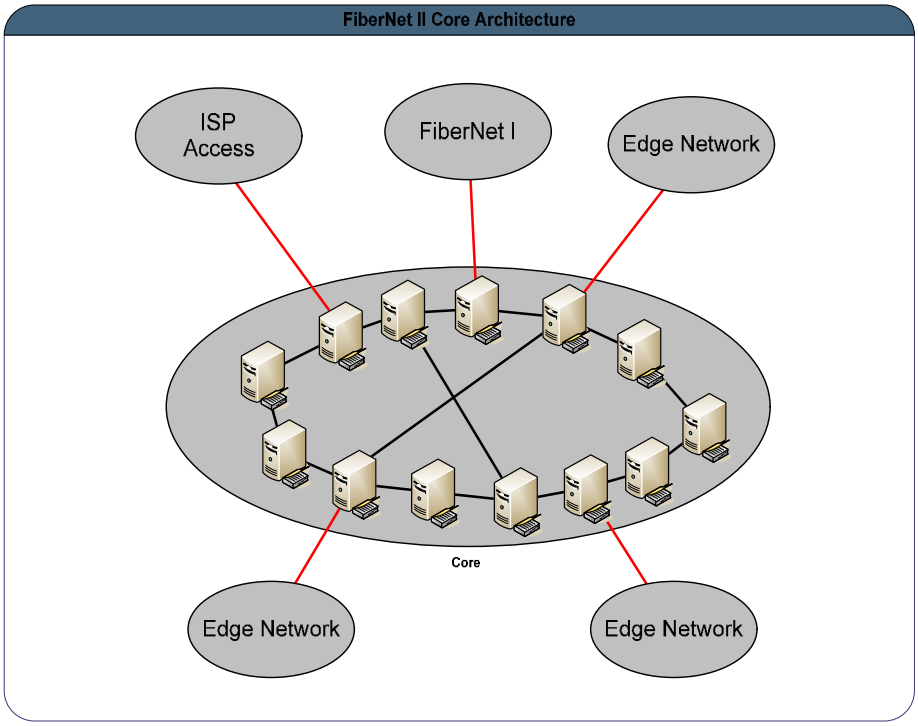


Figure 3.8

The core of FiberNet II is built around a number of 6509 CISCO Routers in a partially meshed configuration where on average every node on the backbone is connected to three neighbor nodes. These form the backbone of the county's MPLS/VPN infrastructure. Customer edge networks are attached to one of the core routers over a fiber optic or frame-relay link.

FiberNet II Edge Architecture

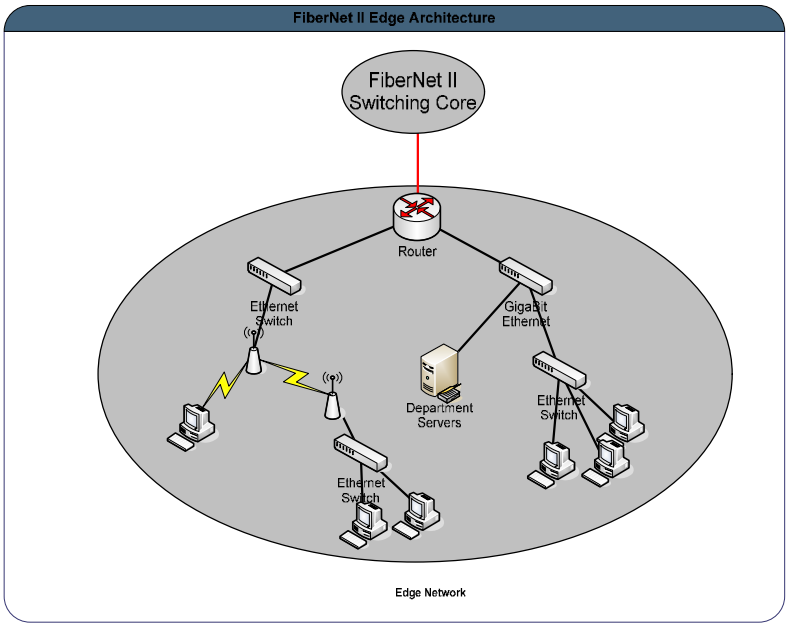


Figure 3.9

FiberNet II departmental edge networks are based around Ethernet and wireless technology. Employees in county offices attach to a local area network through either 802.11 wireless access or direct access to a local Ethernet switch. The county uses CISCO switches and routers to build out their local area networks. Switches are VLAN capable. Where necessary, MPLS capable routers provide the ability to segregate collocated departments and workgroups that will be mapped into departmental IP networks. The edge networks are connected to one of the backbone routers in the core network.

FiberNet Wireless Access Architecture

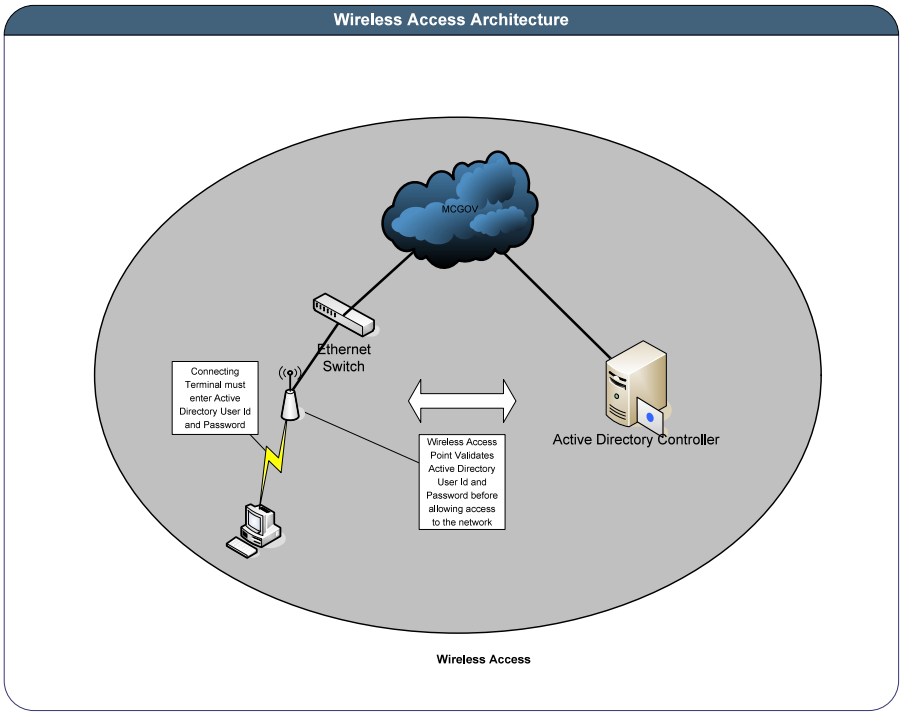


Figure 3.10

In addition to wired technology the county has deployed a large WiFi network. Wireless access is provided in many places via 802.11 b/g/n Cisco access points. The County has deployed Cisco's Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) as its security solution. EAP-FAST is a publicly accessible (RFC 4851) IEEE 802.1X EAP type developed by Cisco Systems. Authentication of a connecting workstation is made through a dialogue with the county's Active Directory infrastructure (see section 3.1 – Active Directory (AD) and Single Sign On (SSO) Services). If the user fails to provide a valid Active Directory login, the workstation is prevented from joining the network.

EAP-FAST has addressed many of the outstanding security issues related to wireless solutions. It provides protection from a variety of network attacks, including man-in-the-middle, authentication forging, weak Initialization Vector (IV) attack (AirSnort), packet forgery (replay attack), and dictionary attacks. EAP-FAST uses symmetric key algorithms to achieve a tunneled authentication process. This tunnel establishment relies on a Protected Access Credential (PAC) that can be managed dynamically by EAP-FAST through an authentication, authorization, and accounting (AAA) server. With a mutually authenticated tunnel, EAP-FAST offers protection from dictionary attacks and man-in-the-middle vulnerabilities. Additionally, the central administration of wireless security enables the County to add users, and to limit their access to specified wireless networks throughout the County's wireless infrastructure.

FiberNet ISP Access Architecture

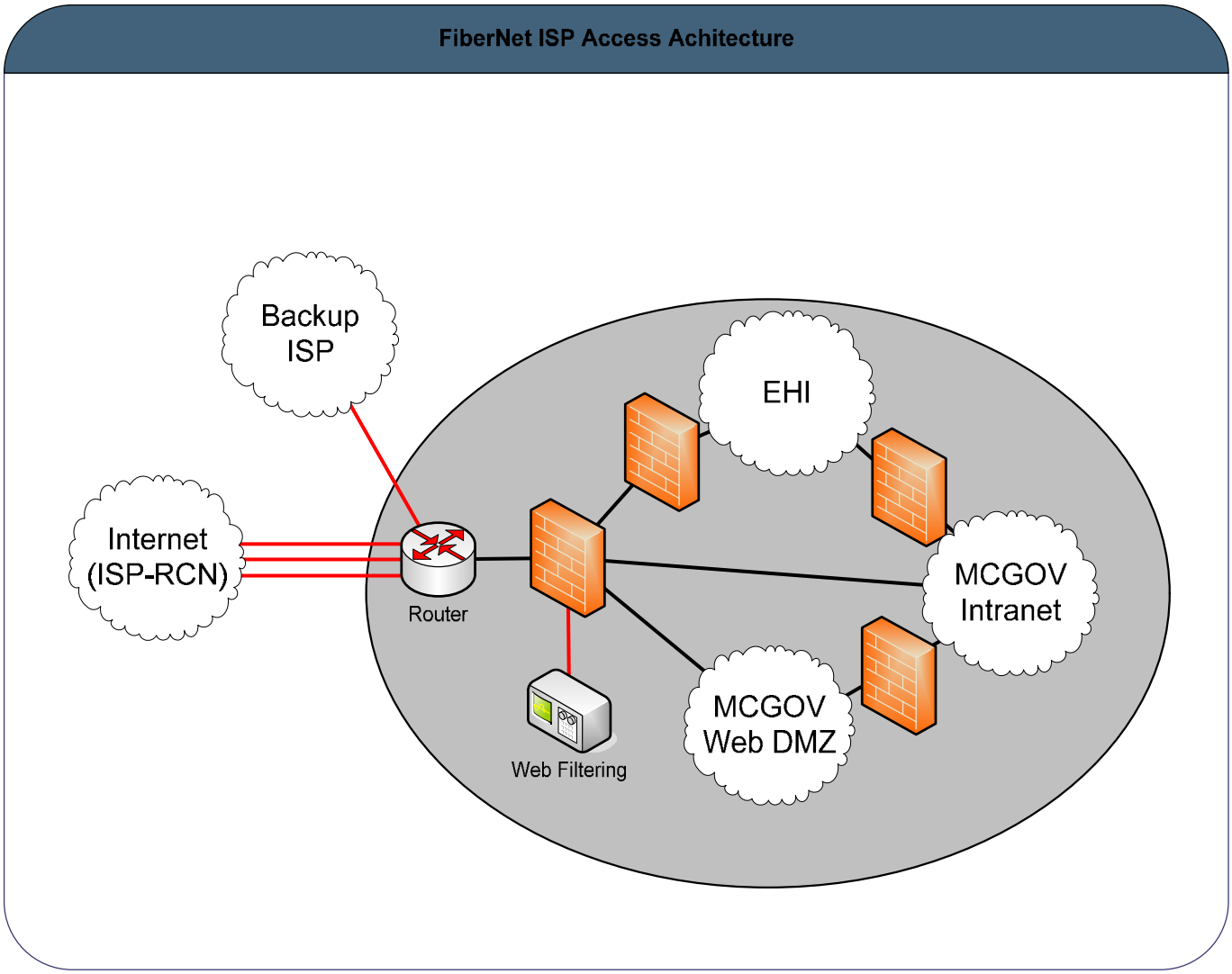


Figure 3.11

Internet access is provided by RCN over multiple T3 circuits that are multi-homed into the county network for load-sharing, redundancy and resiliency. All traffic that enters and exits the county passes through a stateful firewall. Outbound HTTP traffic is filtered through the DTS Security Team's Web Filtering system (See section 3.3 – Security Domain).

The County is working with a second local ISP to multi-home the County's Internet connection. This backup path is available in the event of a RCN failure.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Link Layer Protocols including wireless
Routing & Switching
Perimeter & Internal Security
Network Management
Project Management
Optical Plant Design and Networking
Customer Satisfaction & Support
Network Design

Standards and Guidelines

The County will introduce additional or new standards-based technologies, as these are required. Cost justification of technology is of paramount importance in our decision making process. New technologies must meet the County's architecture goals and must make sense economically. See Table 3-12 for Primary Standards

Table 3-12

IETF Standard/Protocol	Title/Name	Comment
RFC 768	UDP	User Datagram Protocol
RFC 791	IP	Including IP routing processes
RFC 792	ICMP	
RFC 793	TCP	Transmission Control Protocol
RFC 826	ARP	Address Resolution Protocol
RFC 1918	Address Allocation for Private Internet Space	Network Address Translation is used to permit RFC 1918 address to communicate over the Internet.
RFC 2131	DHCP	IP address management
RFC 2362	PIM/SM	Multicasting
RFC 2390	Reverse ARP	Reverse Address Resolution Protocol
RFC 2571 through RFC 2580, inclusive	SNMP	Network Management
RFC 2547bis	MPLS/VPN	MultiProtocol Label Switching/Virtual Private Networks
RFC 4851	EAP-FAST	802.11 security protocol developed by Cisco Systems and made available to the general public in RFC4851
IEEE Standard/Protocol	Title/Name	Comment
802.1D	Spanning Tree Protocol	
802.1P	Prioritization	
802.1Q	VLAN	
802.3	CSMA/CD	
802.3AD	Link aggregation	Trunking
802.3U	MAC 100 Base-T	Fast Ethernet (100 Mbs)
802.3X	Flow Control	
802.3FX	Fast Ethernet over single mode optical fiber	
802.3Z	MAC Gigabit Ethernet	
802.5	Token Ring	Being replaced with Ethernet
802.11B/G/N	Wireless LAN	
802.1W	Rapid Spanning Tree	
802.1X	Port Based Network Access Control	One of the elements supporting Extensible

		Authentication Protocol (EAP) used to implement 802.11 security.
ITU-T & ATM Forum	Title/Name	Comment
AAL1	Circuit Emulation Services	Used for TDM based services
AAL2/3	Variable Bit Rate	Voice – G711, etc
AAL5	Unspecified Bit Rate	Data
PVS & SPVC	Permanent & Switched Virtual Circuits	

Performance

Network performance is monitored continuously in the optical core, and at the client edge. Network Services has developed an integrated Network Management System using standard based tools like HP Network Node Manager, Statseeker and IBM Netcool. Network devices are configured to send SNMP traps when faults or changes in the network occur. These are parsed, filtered and forward to the Data Center and Network Services team for evaluation and resolution. This system is under constant development and improvement.

Capacity planning is performed periodically to determine whether or not a traffic bottleneck is causing congestion in the network. Statseeker is used to track bandwidth utilization and system availability. Reports are reviewed on a weekly basis to look for developing problems and to analyze problems as these are reported.

In general, site to site response times across FiberNet vary depending upon the time of day, inherent delay, and latency in the traveled circuit. Observed ping response times between sites on the fiber-optic network range between 1 to 3 milliseconds (ms). Adding frame-relay to the traveled circuit adds another 3 to 4 milliseconds, and adding a wireless link adds another 1 to 4 milliseconds. During normal network operation, ping response times are usually below 11 milliseconds, from edge to edge. Network throughput is governed by the most restrictive carrier link in the circuit. FiberNet uses circuits ranging from 10 gigabit/second to 10 megabits/second for Ethernet links and 1.544 megabits/second for frame-relay. Contention and congestion affect throughput and must be considered when designing applications. Each media and every component in FiberNet is shared by every active application traveling a particular communication channel.

Reliability

At the physical layer, reliability has been achieved with redundant components like multiple switches and power supplies, multiple and diverse fiber paths, and uninterruptible power supplies (including dedicated generators) within the supporting infrastructure. FiberNet I and FiberNet II use a partially meshed backbone design. Every FiberNet Hub has at least two diverse links (east-west) attaching to its nearest neighbor. In most cases, there are three links. At the next layer in the OSI model, reliability has been engineered into the electro-optical network core with the use of multiple technologies. On FiberNet I, ATM is the logical link layer protocol . ATM Permanent Virtual Circuits (PVC) and Soft PVCs provide circuit protection by supporting multiple paths to very destination. FiberNet I is a Layer 2 network, recovery from a network fault happens at the Logical Link Layer. On FiberNet II, the same partially meshed backbone provides protection from backbone link failures. FiberNet II is fundamentally a Layer 3 network topology. Fault recovery is performed in the routing plane of the network. This design removes the single point of failure flaw in the FiberNet I.

The County maintains an inventory of spare equipment. Equipment from this inventory is used to quickly replace failures at edge sites and in the core. FiberNet/WAN was designed to transport public safety applications. For this reason redundancy, robustness, proactive monitoring and management have been design requirements from the beginning. The core and the customer edge sites are monitored 24 hours per day, 7 days per week. Field engineering is available within a two hour response time, and all outages are treated as major outages. Service Level Agreements stipulate an eight hour time frame for repairs to electrical component faults. Fiber repair times are more problematic due to external forces like hurricanes, snow storms, thunder storms and accidents. Our experience has been favorable; these types of failures and long-lived outages have been rare.

Availability

The County tracks availability statistics for FiberNet's backbone, and user sites separately. Average availability over the most recent quarter has been 100% for FiberNet's backbone and 99.9% for all user site outages. Public safety and other important sites which operate on a 24 hours, 7 days per week basis receive 2 hour on-site response times with 8 hours as the targeted time to repair for equipment related faults. Most user-site outages are related to local power failures and the recovery there from. Such outages do not reflect upon the stability and reliability of FiberNet core; rather these indicate the assessed criticality of the user site. Sites are not public safety sites or other critical sites, and do not operate on a 24 hours per day, 7 days per week schedule. These are sites closed on the weekends and after 6:00 PM, forcing repairs efforts to wait until the site is accessible.

Security

Although security is addressed as a separate topic within this document, it is also a design goal within the network infrastructure. FiberNet's circuits are inherently secure. Desktop and server connectivity is provided through switches. The County does not use shared media hubs to deliver services. This design principal mitigates the risk of network sniffing and man-in-the-middle attacks. FiberNet is also concerned about the security and survival of its physical infrastructure. FiberNet has added and will continue to add external physical security, fire suppression, environmental monitoring and control systems to this infrastructure.

Management systems and protocols are often a security risk in a large network. The management core for FiberNet is not accessible from the County network and the Internet. Network Services maintains a logically separated NMS network to monitor the networking infrastructure. There is no dial-in capability within the WAN.

Internal security for the network is provided by several firewalls that provide "security in-depth" for the County's IT assets. Internet access is mediated by high-availability firewalls that screen all traffic. Additionally, dedicated internal firewalls segregate special purpose networks from the main County network.

Wireless access to the county network is protected by the use of an Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) solution.

Wireless Access

The Network Services team must specify and install all wireless access points attached to the County's networking infrastructure. Wireless access points must follow the County's architecture and standards. Fundamentally this means using EAP-FAST for authenticating to the county Active Directory. In rare circumstances, Network Services has deployed ARUBA access points for special applications. We fully

anticipate deploying ARUBA access points to support AVAYA 802.11 wireless phones connecting to the County's PBX.

Network Services is currently looking into 802.11n technology as the next generation of WiFi for the County. This technology may enable the County to stop placing data networks in offices.

Internet Access

The Network Services is responsible for protecting the perimeter of the County's network as well as providing security in depth; where it is required. Concerning Internet access, Montgomery County Governmental access to the Internet must pass through designated border routers and firewalls maintained by DTS. Any Internet connection that is not maintained by DTS is considered to connect to a foreign network. The Internet attaching network will not be permitted to connect directly to the County's network. Examples of this type of connection are the Department of Public Libraries and the DOT/Advanced Traffic Management network. Each of these networks connects directly to the Internet without going through a DTS maintained firewall. However, each of these networks in turn connects to the County network through a stateful firewall this is maintained by Network Services.

New Applications or Services

New applications or services must use IP based communications for their Network Protocols, conform to industry best practices and comply with the County's Security Policy as well as legal mandates and contractual obligations entered into by Montgomery County Government, e.g. PCI.

Disaster Recovery

The Network Domain is the most basic IT Service within the County. Almost all Enterprise Services depend on the Network in one form or another. A number of disaster recovery strategies are employed in the Network Domain to avoid and recover from failure such as:

- Multi-homed ISP connections - in the event of one ISP failure the other will take the load.
- Fibernet II is designed with a partially meshed backbone which provides protection from backbone link failures.
    - FiberNet II is fundamentally a Layer 3 network topology.
    - Fault recovery is performed in the routing plane of the network.
    - Fibernet II does not have a single point of failure.
- The County maintains an inventory of spare equipment. Equipment from this inventory is used to quickly replace failures at edge sites and in the core.
- Core and customer edge sites are monitored 24 hours per day, 7 days per week. Field engineering is available within a two hour response time, and all outages are treated as major outages. Service Level Agreements stipulate an eight hour time frame for repairs to electrical component faults.

The Network Domain offers a critical Disaster Recovery service to the Deployment Domain. The Network Services Team supports the ability to drop a deployment zone in one data center and bring it up in another data center. This allows the movement of VMGuests with their IP addresses from one data

center to the working data center. This avoids many Application, Database, ESB exchange, and firewall rule configuration issues.

See the Disaster Recovery Domain for information around prioritization of services and policies.

3.13 PBX Network Domain

Principles

The PBX Network Domain provides advanced voice services for most of the County Executive Branch Departments. The DTS PBX Telephone Services team provides the following services:

- Legacy Voice Services
- VoIP Services
- Voice Mail
- Management of the connection and agreement with the County ILEC
- Maintenance of the County Phone Directory – both online and printed
- Maintenance of the County's 311 connection with the various Telecommunications providers servicing in the County
- Maintenance of the endpoint switches with select departments including MC311
- Maintenance of a backup switch for critical phone numbers

The County maintains a modern Avaya Communication Manager that leverages the Network Domain (see section 3.12) to provide the above services. Communications Manager is a highly reliable and scalable system that provides access between voice and data endpoints.

The DTS PBX Telephone Services team supports both legacy voice and newer VoIP services. New installations are now being installed as VoIP services. The Communication Manager system supports both the old legacy voice and the newer VoIP services, enabling the County to continue to leverage its investment and allocate funds for new locations and new applications.

Select departments such as MC311 have their own Avaya endpoint switch. The PBX Network team supports the endpoint switches and their connection to the main Avaya Switch.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS PBX Telephone Services Team.

Components

The Avaya Communication Manager is a highly reliable and scalable system that supports digital voice, video and data communications and is designed to meet the County's information movement and management requirements, both today and in the future.

The platform provides an open architecture; conforming to QSIG, TCP/IP, ISDN BRI, TAPI, TSAPI, JTAPI, ASAI, LDAP, H.323, and H.248 standards. This translates into better integration and an increased number of high quality applications.

Avaya Communication Manager combines the legacy architecture of its predecessor, Definity ECS, with the IP Telephony Standard H.323 Media Server/Media Gateway architecture. This enables the County to leverage its current infrastructure and minimize capital outlays. With Communication Manager, Definity ECS Expansion Port Networks (EPNs) become Media Gateways that communicate with new S8720 Media Servers via IP addresses. The existing cabinets and cards continue to provide service, enabling the County to continue to support legacy requirements for as long as needed. New media gateways are added as either chassis based G650s or H.248 switches that have call processing elements built in. IP endpoints can be supported from either the legacy gateways or the newer H.248 gateways. All of the capabilities and features that previously existed in the system carry forward to the new gateways. And new features and capabilities are now available to existing users as well.

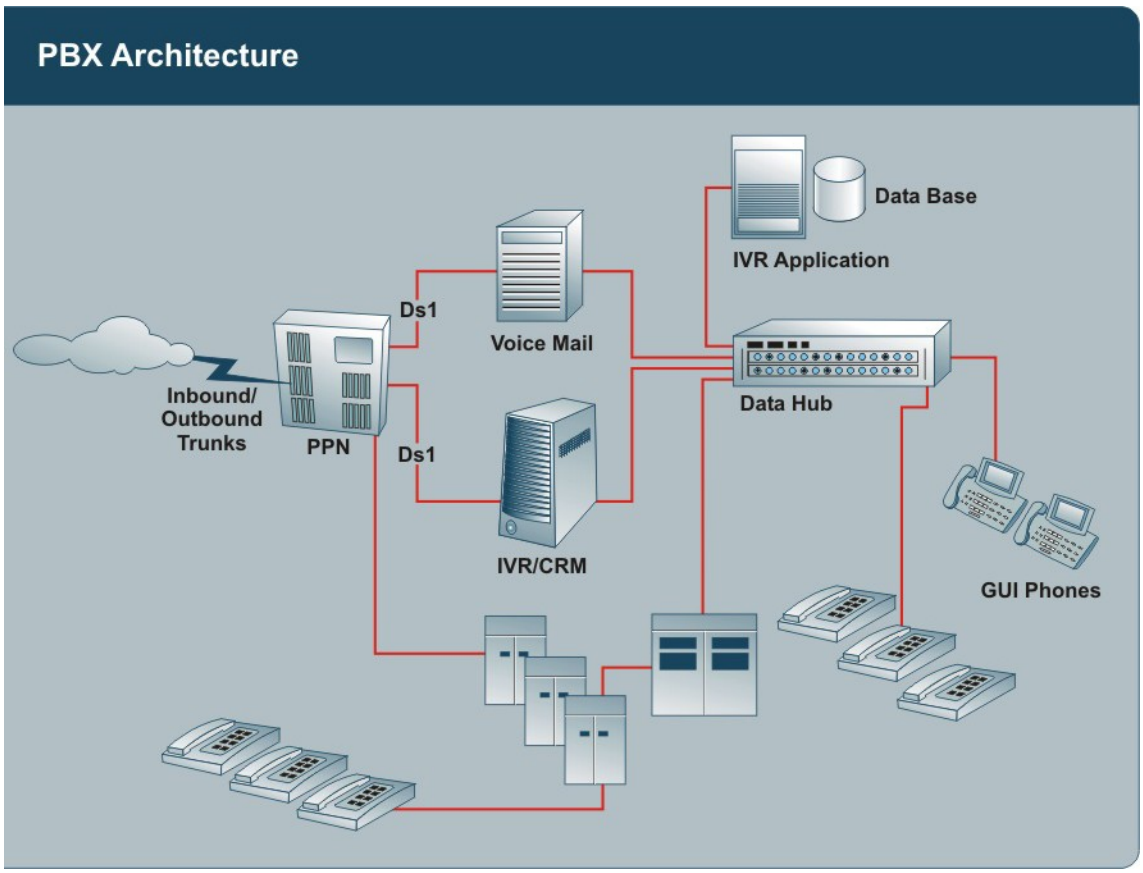


Figure 3-13 PBX Network Domain

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
PBX System Administration programming
Network wiring techniques
Call Center Vector programming
PBX network Design and Installation
VoIP

Standards and Guidelines

- The County conforms to security standards for G3r systems as outlined in the Avaya Toll Fraud and Security Handbook [2]
- All new endpoints are added as VoIP
- Critical Phone numbers are identified through department's telephone services administrators. The PBX Network team uses a backup switch during critical failures and during switch maintenance to keep these numbers operational.

Disaster Recovery

The PBX Network team has a number of Disaster Recovery solutions in place. The first solution relies on 24x7 monitoring support from Avaya and maintenance by the DTS PBX Team of an On Call PBX Administrator who is informed of any outages by Avaya. The On Call PBX Administrator determines the severity of the outage and manages the resolution of the issue.

To maintain availability of critical telephone numbers the PBX Network Team has a backup switch that can support the critical phone numbers during periods of switch maintenance or critical failures.

Finally, departments like MC311 who have their own endpoint switch are connected to the main County PBX switch. Disaster recovery support can be provided on a case by case basis with the department whereby the failure of the endpoint switch or the main County switch can be recovered through the other switch. In the case of VOIP phones the phones can be configured to failover to the other switch for services during a failover. Ability to dial out is maintained with the ability to accept incoming calls requiring additional support which is again provided on a case by case basis.

[2] Avaya Inc., *Avaya Toll Fraud Security Handbook*, May 2003

3.14 Record and Document Management Domain

Principles

The Record and Document Management Domain is Montgomery County's integrated, comprehensive enterprise approach to centrally administer and manage all county electronic records.

The Records Management function for Montgomery County is the responsibility of the Department of General Services (DGS), Division of Real Estate Management Services Section. They own the responsibility for Records Management in the County which includes both physical and electronic records. They define the policy the county will follow, enforce the policy, provide education on the policy, define the tools (warehouse and IT) that will be used to implement the policy, etc.

Records Management is a management discipline that is responsible for the control of official records. It is a methodology for defining important records, their safe storage, how they can be used, how long they must be retained, and when they can be destroyed. A data retention policy is an important aspect to the Records Management function.

The DTS Core Systems team supports their IT Requirements by maintaining a Document Management/Imaging solution. The solution accommodates records from virtually any source, including scanned documents, electronic files (e.g. Microsoft Word, PDF, JPEG, etc), e-mails and attachments, COLD reports and other business applications.

The Document Management/Imaging function is integrated with Records Management which manages the life cycle of the records. The records are kept in the system during the active period when records have the operational value. The inactive records are archived for records management in accordance with the retention policy.

DTS will maintain a Record and Document Management section on the DTS departmental homepage on the Intranet Portal. The Record and Document Management section will contain information about the service as well as an intake form and a roles and responsibility document. Finally, it will contain a directory listing for the electronic Records and Document management sites.

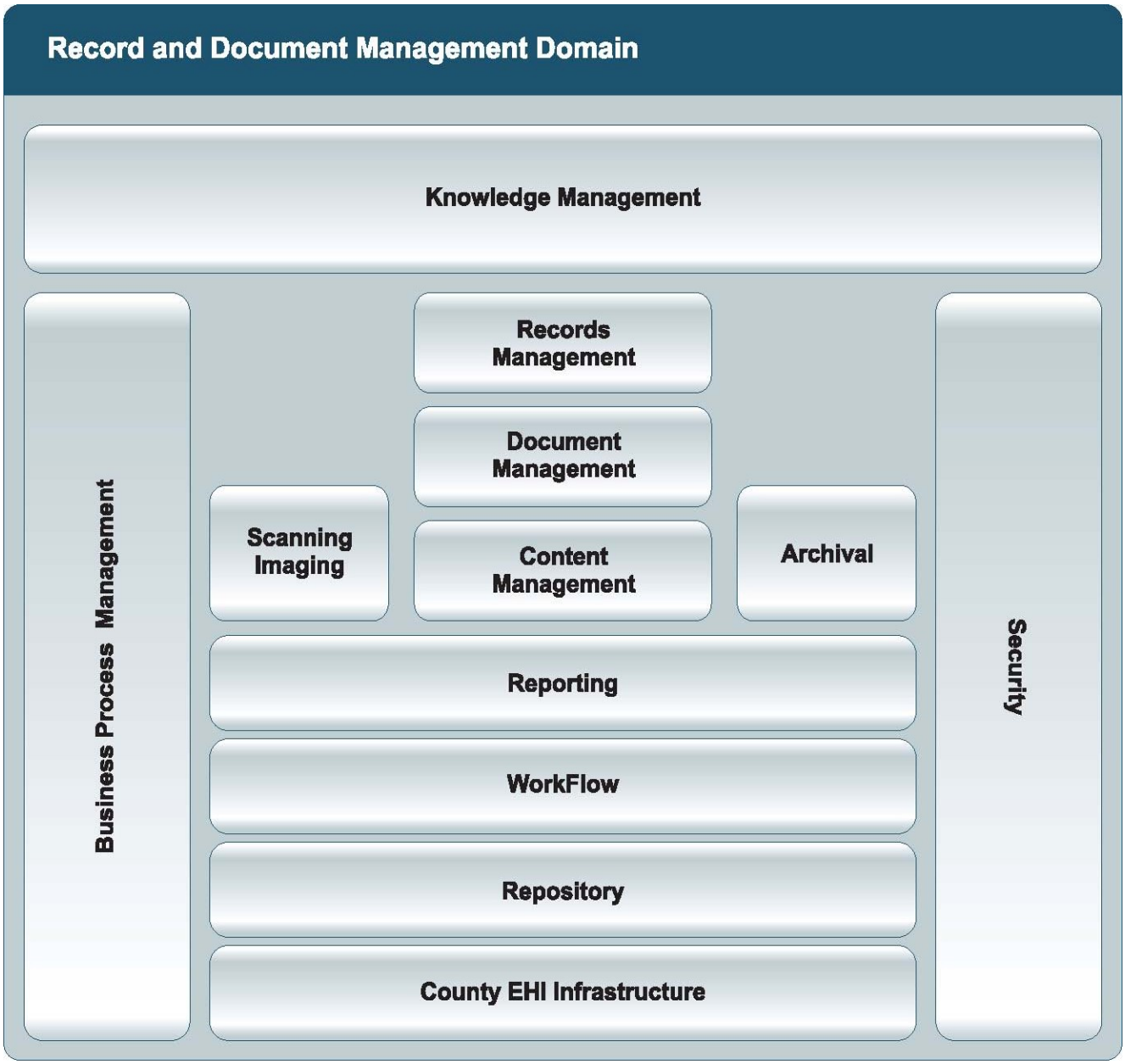


Figure 3-14 Records and Documents Management

Owners

Business Owner

The business owner for this Domain is DGS's Division of Operations Support Services Section.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

The DTS Core Systems Team supports the ZyImage Enterprise Web Server for storage of electronic records and documents. The ZyImage Enterprise platform provides functions for office workers to capture, manage, publish, share, and archive information throughout its entire lifecycle in a single document repository. It is designed for performance, flexibility, and reliability.

The ZyImage system leverages the other Architecture domains including the Deployment Domain (see section 3.4), Network Domain (see section 3.12), Help Desk (see section 3.9), Active Directory & Single Sign On (see section 3.1), Service Enabled Domain (see section 3.16), Enterprise Server Management (see section 3.20) and System Operations Domain (see section 3.17).

When groups are given access to the system their area and content are restricted to an Active Directory group that is under the control of their Department. The owning Department controls membership within that Active Directory group.

The platform has an open architecture, conforming to standards like ODBC, LDAP, Active Directory, TCP/IP, XML, COLD, .NET, and NARA/ERA and offers a robust fuzzy search and retrieval engine. System integration can be done through common gateway interface (cgi) coding to integrate with Microsoft office applications and web applications, or ZyImage Application Integrator. ZyImage accommodates records from virtually any source, including scanned documents, electronic files (e.g. Microsoft Word, PDF, JPEG, etc), e-mails and attachments, COLD reports and other business applications and synchronizes with databases like Oracle, SQL and Access.

The following modules are major ZyImage elements working together to support the enterprise document management and records management need:

- Zyscan converts paper documents and existing image formats into searchable online information. By digitizing the paper documents into electronic format, records become searchable.

- ZyIndex converts and manages scanned and electronic information. This module has a timer program to index all data collection. It also creates web clients for different applications.

- ZyCold automatically converts digital spool files into ZyImage searchable files, and adds key fields for key-field search and full-text retrieval.

- ZyImage for Forms interprets all common types of characters in paper forms, whether they are machine-print (OCR), isolated handprint (ICR), alpha and numeric mark sense (OMR) or bar codes.

- Records Management and Archival plug-ins enable storage of documents into a data repository from County standard desktop applications such as Microsoft Outlook, Microsoft Word, Microsoft Excel, Microsoft Internet Explorer and Adobe Acrobat.

- ZyFind allows searching, finding and organizing the documents in the data repository.

- ZyPublish copies data onto a CD or a DVD, and makes the data searchable.

- ZyImage webserver allows users to share indexes and data over the intranet. Using the browser, authorized users can search information.

- Records Management converts ZyImage into a record-management system and allows users to

manage and search records.

- Document Management adds the additional functions of version control and check-in/check-out, to enable multiple users to work on the same set of documents. This module integrates with Microsoft Office XP applications.

- Workflow allows users to route documents through an organization, according to a specific pre-defined path.

- Audit Trail stores all user activities (such as searching, viewing and editing documents and opening, deleting, and building indexes) in an XML file.

- Advanced Security modules provide document-level security options. The document groups are based on the contents of key fields and protect documents from unauthorized access. The system looks up users in Active Directory and set security rights for specific functions such as building, deleting, and creating indexes and editing, deleting and merging documents.

- Bates Stamping module provides every document and page a unique identifier which can be placed on the original images during the ZyFind export or printing process.

- XML Wrapper modules generate a universal key field structure over scanned paper and electronic file formats. This module connects electronic files to an XML file containing key-field information.

- Application integration enables ZyImage integration with other systems. This module will enable the County to integrate with other business applications.

- ZyAlert modules enable selective dissemination of information. It automatically detects relevant information in huge indexes and sends notification when the requested information is found. This module acts as an information agent which searches the data at set times, based on user profile.

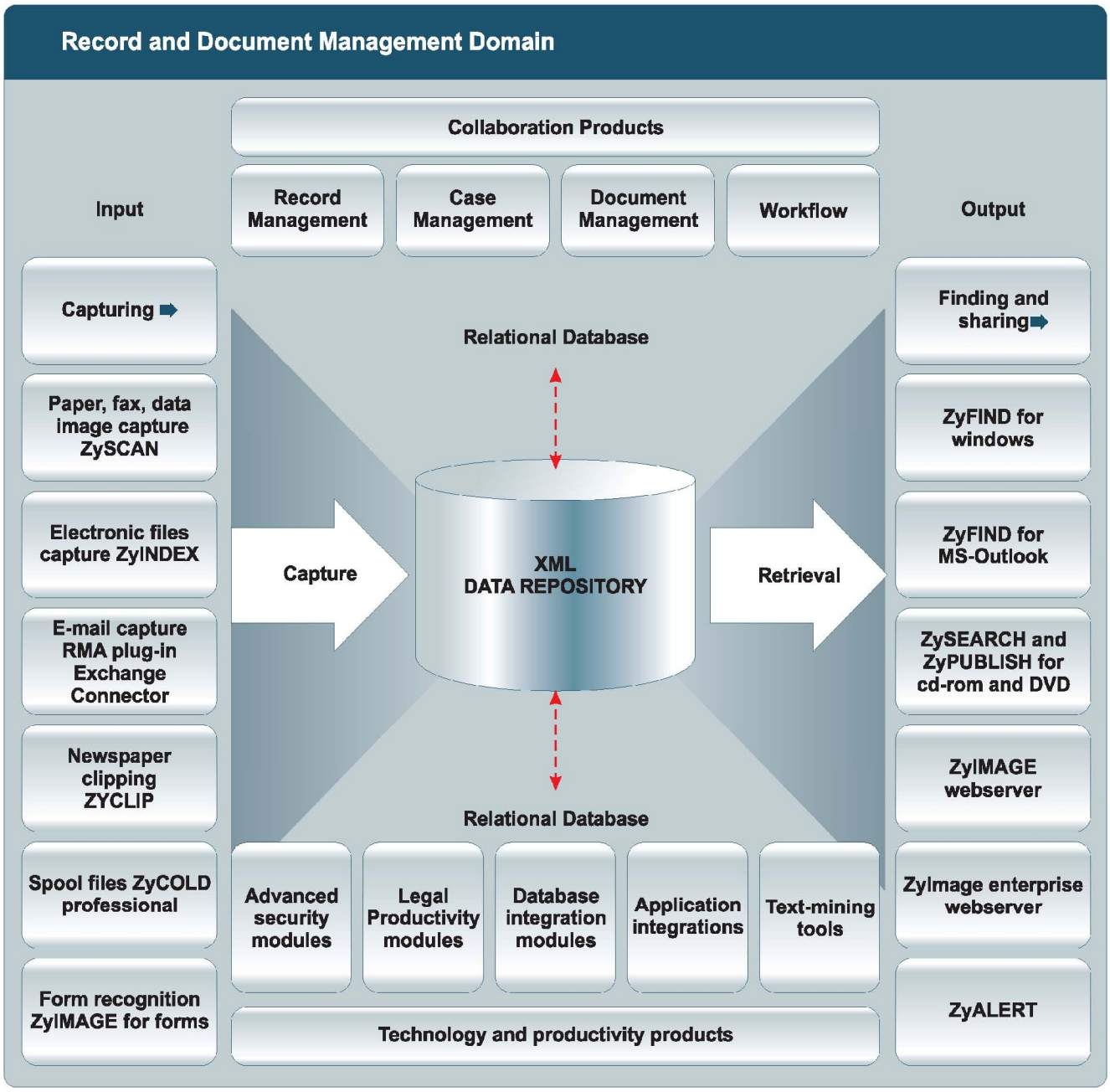


Figure 3-15 Record and Document Management Domain

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Microsoft Windows Operating system knowledge and experience
Microsoft Windows Applications
Data Base Management - Oracle and Microsoft SQL knowledge and experience
Records Management

Visual Basic
Networking
Active Directory
HTML, XHTML
XML, XSLT
Java
ASP.Net
SOAP

Standards and Guidelines

The County needs to comply with the rules and regulations of Montgomery County, the State of Maryland, and the Federal Government. Some of the standards that must be taken into account are HIPAA, Sarbanes-Oxley and COMAR 14.18.02 to 14.18.05 to ensure that vital records needed for business purpose are retained, organized, protected and searchable. The following guidelines should be applied to a document before it enters records management**.**

- Inventory the records (the official documentation of business activities)
- Categorize the records generated. State laws allow records to be grouped into categories (contracts, personnel records, etc.).
- Prepare the metadata, or taxonomy so that the records can be searched
- Consider the format of the electronic data
- Identify the employees responsible for maintaining the record
- Preserve the data and determine how long specific types of records should be maintained.
- Manage hardcopy and electronic documents (including computer generated documents and email)
- Give instructions for disposal of certain records, and update the retention schedule
- Establish procedures for ensuring compliance with the policy
- Enable historical preservation of the County records if it is required
- During litigation:
    - Provide documents and preserve evidence to support positions in litigation
    - Suspend the destruction schedule
- Permit the disposition, discard unnecessary records, and reduce storage costs.
- Comply with federal laws and state-specific requirements
    - COMAR (Code of Maryland Regulations 14:18:04 Electronic Records)
    - HIPAA (Health Insurance Portability and Accountability Act)
    - MPIA (Maryland Public Information Act)
    - NARA/ERA (National Archives and Records Administration/Electronic Records Archives)

Record and Document Management Intake Form

- A requesting team or department must fill out a Record and Document Management Request Form.

Collaboration Agreement

- A requesting team or department must read and agree to the Record and Document Management Agreement. The Record and Document Management agreement lists roles and responsibilities

for the service.

Records Management Administrative Procedure

Montgomery County Office of Management and Budget – Administrative Procedure 6-3, September 8, 1975; *Records Management Addendum*;

3.15 Reporting Domain

Principles

The County uses the Crystal Reports package to meet its diverse Enterprise Reporting requirements. The County uses Crystal Reports because it offers distinct capabilities and optimizes the use of software licenses.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

Crystal Reports will be used to develop reports to various data sources, including On-Line Transaction Processing (OLTP) systems. Crystal Report is comprised of the Crystal Reports Designer (CR) and Crystal Enterprise Server (CE). CR is used for report development and is a package which installs on the developer's desktop. Its design allows for control over data access and presentation and offers a variety of formula functions, operators report formatting, complex logic, and data selection. Once developed, the report is then made available or "published" to the CE server.

The CE server is a web-enabled server, which runs on the Windows operating system. Connectivity to all data sources is through Open Data Base Connectivity (ODBC). Current data sources are Oracle, MS Access, Mainframe-based DB2, PC-based DB2, and MS SQL Server. Other standard data sources are supported. The County is licensed for unlimited connections, and currently hosts 1,500 clients and 2,400 reports. Access by other non-County government entities is provided. The CE server is very scalable, and allows for specific growth options as required.

Clients access the published reports through a desktop client browser from the CE server. Additionally, several applications have been developed in-house which call CR reports directly from the server, bypassing all direct user input. J2EE is the standard application development platform. CE supports Single Sign On by authenticating users with the County's Active Directory (AD). Security for report access is based on individual accounts and AD group membership. Enhanced security is available and can be applied to users, groups, or reports.

Once a report request has been processed on the CE server, the report can be accessed using the following methods:

- Web browser
- PDF (Adobe Acrobat)
- Excel
- Word

Additionally, reports can be scheduled to run once or on a schedule. Users can view the latest or a previous "instance" of a report. Reports can be deposited to file shares or sent as an email attachment in the desired format. Report parameters can be entered via custom application interfaces or directly by the user. Reports can be integrated and are viewable from within an application.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Crystal Reports Designer
Windows Server Administration
Crystal Enterprise Server Administration
Printer Administration
Network concepts and administration
ODBC configuration management
Active Directory concepts and administration
Relational Data Base concepts
Desktop configuration for Crystal clients
Troubleshooting skills
DBA knowledge and administration

Standards and Guidelines

Policies:

Publishing policies and current procedures can be found in Outlook public folders, MCG, and Crystal Reports.

Standards:

Reports must be tested using Crystal Reports from the developer, then tested using Crystal Reports on the CE server, and then tested in "published" form.

Access to reports must be in compliance with security guidelines. Applications which call published Crystal Reports from the CE server should be developed using J2EE. This will provide for secure transmission of the user name, password, and report contents over the intranet and internet.

The CE reports using mainframe DB2 data must be optimized for performance by the database administrator. To minimize the impact of day-to-day reporting, long, complex, CPU intensive reports are to be scheduled to run during off-hours. This level of access is controlled by the Crystal administrator, who can delegate this authority to departmental IT contacts. View on demand reports are CPU intensive, and have no governors on processing time. They can use all of the CPU cycles, effectively locking out all other report processing. Scheduling uses different CE server components which do not exhibit this behavior. For SAS reports accessing the mainframe DB2 data, optimization must be in conjunction with SAS.

Direct access to the CE server via a Web browser requires AD authentication. For example, to access published Crystal Reports, the requestor must have a user account in Active Directory.

There are two kinds of accounts that access Crystal reports, those which are imported from AD and those which are created on the Crystal Enterprise server. The accounts created on the Crystal Enterprise server are not authenticated with AD, and they do not support Single Sign On (SSO). Applications that directly call reports from the CE server use these accounts. This assumes that acceptable security is provided from the application for intranet-only applications. If it is not provided, the application should be developed using J2EE.

Large additions (more than 50 reports), or major applications that rely heavily on Crystal will be examined for their effects on resources. This will be done to ensure satisfactory performance for existing and new application users. The number of reports, their complexity, frequency of generation, and average and maximum concurrent users will be reviewed. From this, the County may determine the potential effects of change on the CE servers.

DB2 on Mainframe – The County is particularly cautious of performance degradation caused by reports which access mainframe DB2 data. Execution of the report's complex queries can have a significant negative effect on processing resources. This can create problems with the application, and with other applications running in the shared mainframe environment. Similar problems can occur on the Intel Database Servers.

3.16 Service Enabled Domain

Principles

The Service Enabled Domain promotes the development of robust, scalable and flexible services for business integration with the County infrastructure. The goal is to achieve a cooperative and secure service and data sharing environment, and to avoid data replication

The County recognizes the importance of developing Services capable of integration with internal and external systems. These Services will be designed and implemented, based on events and messages. An event-based, messaging model will help avoid stovepipes (rigid, self-contained functionally organized service solutions for each department, not acting as a single-entity). To do this, the County hosts a healthy mix of services. Some have been developed in-house, and some are COTS (Commercial Off-The-Shelf) solutions. Each application will document and publish well-defined interfaces to the protocols identified in this section.

An events-based messaging service will foster the maturation of service implementations based on Service Oriented Architecture (SOA). The County encourages the use of XML to define event messages, Web Services technologies for integrating .NET and J2EE services and Enterprise Java Bean (EJB) for integrating J2EE services. The following table lists the County's supported protocols.

Protocols
Message Q
Enterprise Java Bean (EJB)
Java Messaging Services (JMS)
Service Oriented Access Protocol (SOAP)
Secure Hypertext Transfer Protocol (HTTPS)
Web Services Description Language (WSDL)
Universal Description Discovery and Integration (UDDI)
Representational State Transfer (REST)

Table 3-17 Service Enabled Domain Protocols

Enterprise Service Bus (ESB)

The County has deployed and maintains a distributed event services environment for communications between peer Services. This event service environment uses the SOA architecture pattern called Enterprise Service Bus (ESB). ESB is a specific server implementation of Service Enabled Domain services. ESB provides the feature capabilities listed in table 3-18.

Features
Protocol Switching
Message Routing
Message Transforms

Message Transports
Message Security
Message Aggregation/Splitting

Table 3-18 ESB Feature Capabilities

ESB provides a rich, event-based messaging infrastructure that aids the implementation of complex Service Enabled Domain Services and client consumers. Figure 3-19 shows a modular overview of the ESB.

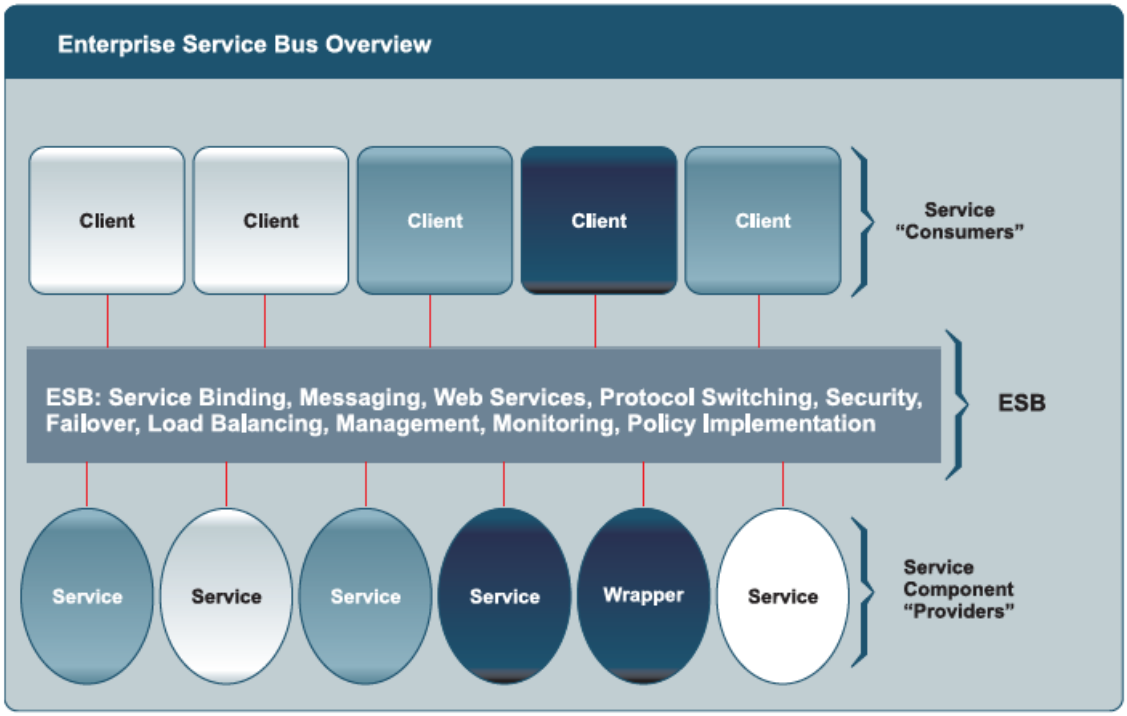


Figure 3-19 Enterprise Service Bus Overview

Compared to a home-grown Service Enabled Domain hosting environment, the standards-based ESB provides extreme flexibility for future integrations and extensibility.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Enterprise Services Architect.

Components

The County will deploy a distributed environment for communications between peer Services. With the development of a robust collection of Business Objects, their Service Interfaces and bindings will expose functions to other applications. Figure 3-20 shows an integration scenario for Services using ESB.

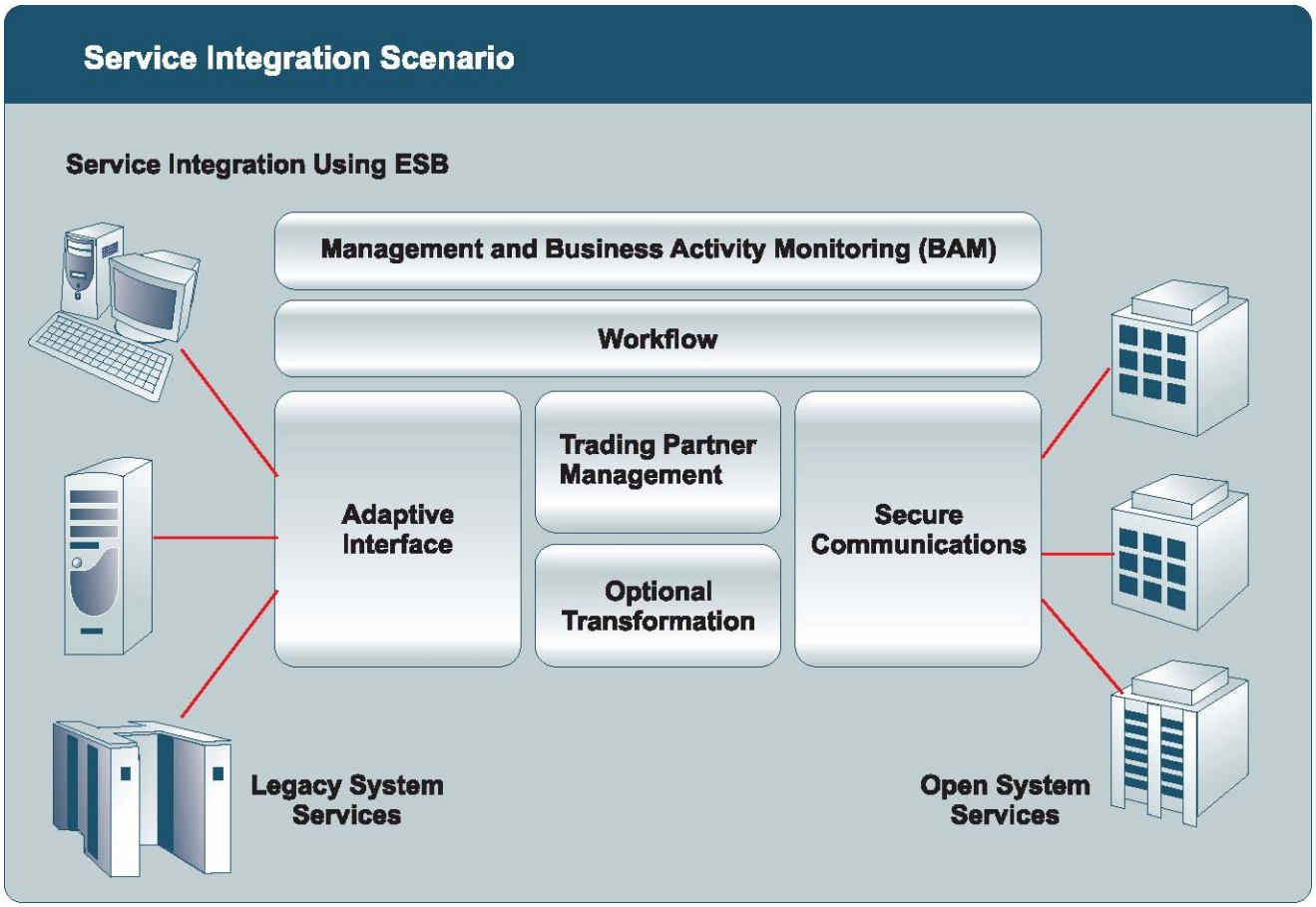


Figure 3-20 Service Integration Scenario

As Figure 3-20 shows, the County encourages the development of wrapper services for legacy system services. This is to enable legacy implementations to participate in event-based Service Enabled Domain.

The County encourages Service providers and consumers to document the message structure, format, data requirements, and security requirements. It also encourages documentation of the event generation, flow, security, and other SLA requirements. For secure communications, the County is using messaging protocols such as HTTPS (for Web services, and normal web calls) and JMS on WebSphere MQ (channels secured as needed). Business Objects may be implemented as EJB, Message Driven Beans or Java objects.

To accommodate diverse technologies, the County recognizes the value of a Service Oriented Domain, and plans to develop an infrastructure to support Web Services . The County encourages Services to be implemented to comply with industry-published standards and specifications like the Web Services –

Interoperability Basic Profile (WS-I BP), which minimally includes vendor-neutral components such as SOAP, WSDL, UDDI and XML and XML Schema.

Security issues are associated with Web Services and other messaging services, and the County will proceed with caution as the technology matures. The County strongly recommends encryption of data in transmission. Upon review of a service and the content of its messages, the County may mandate data encryption. The ESB platform which the County hosts contains a standard set of data encryption capabilities, such as PGP. The County will reserve the right to review the publication of Services (via JNDI or UDDI) both within and outside its Intranet boundaries. Data transmissions to and from systems external to the County will be reviewed and approved on a case-by-case basis.

The County will encourage data transmission in XML format (where the technology permits), particularly in domains where industry standards exist. The County views XML as the interoperability "glue" that allows systems being developed to communicate with each other. It paves the way for future expanded collaboration. This XML data transmission architecture is technology independent, therefore it will work with both J2EE and .NET protocols. Also, XML data transmission architecture on an ESB platform provides a seamless mechanism to transform message data for the requirements of other services and consumer clients. The following Figure 3-21 demonstrates the County's Service Enabled Domain.

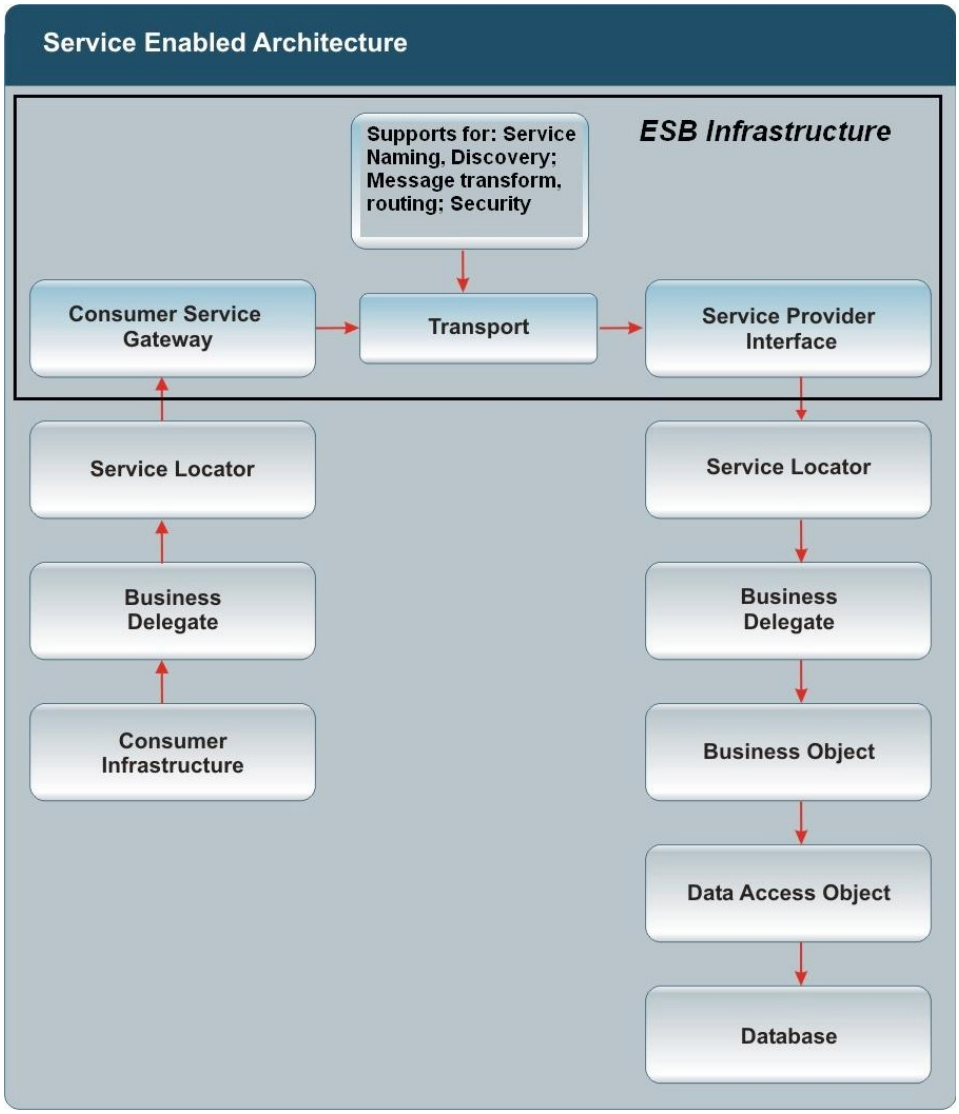


Figure 3-21 Service Enabled Domain

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
WebSphere MQ
Java Message Service (JMS)
Enterprise Service Bus (ESB)
Web Services
Enterprise Java Beans (EJB)
Simple Object Access Protocol (SOAP)
Representational State Transfer (REST)
XML
XSL Transformations (XSLT)

Standards and Guidelines

The County has standards for Java files to have following package structure:

gov.montgomerycountymd.<<dept>>.<<application>>.<<module>>

where

dept will be the short name of the department that owns the application
application will be the short name of the application itself
module will be the implementation section.

The County has standards for .NET namespace:

gov.montgomerycountymd.<<dept>>.<<application>>.<<module>>

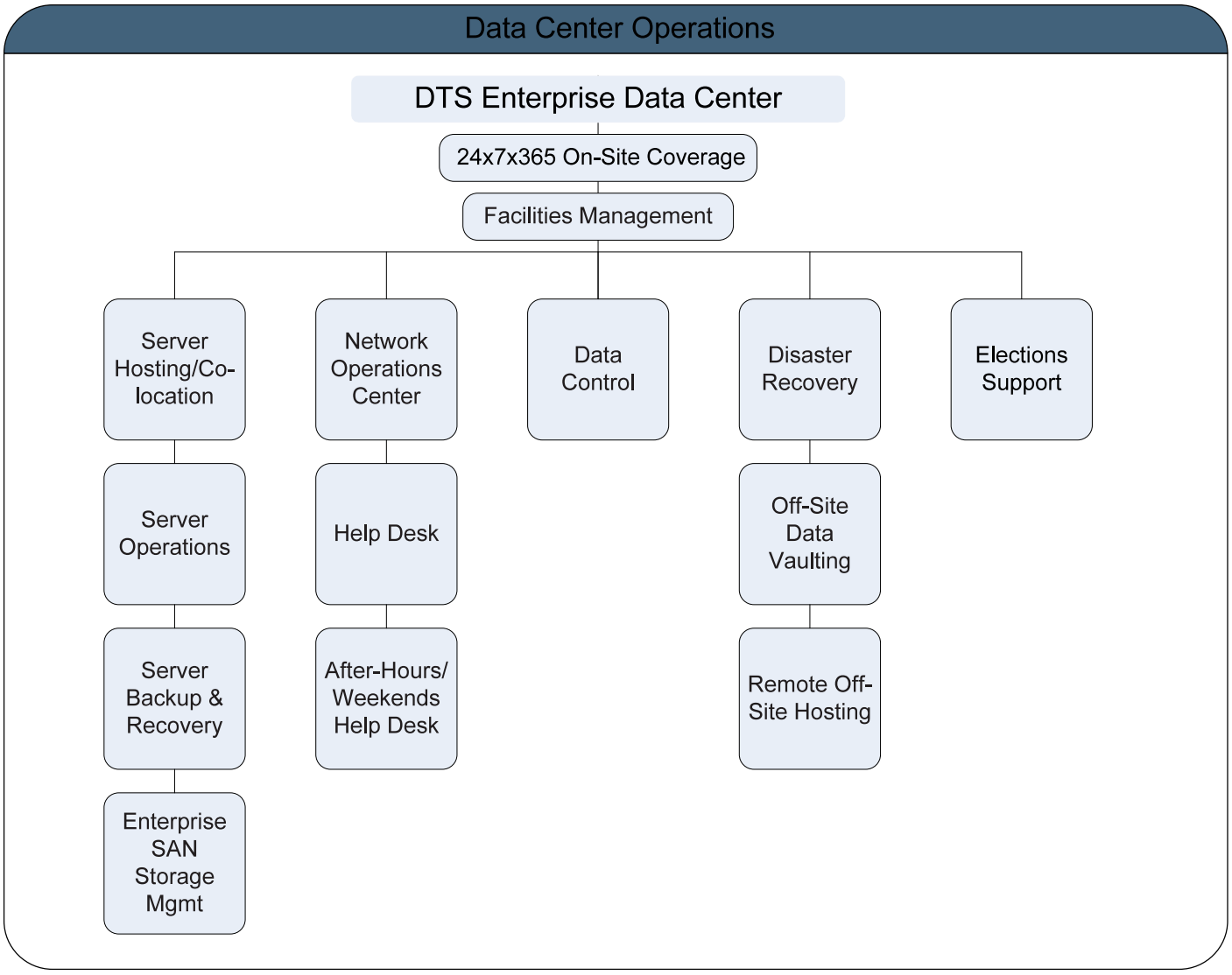
where

dept will be the short name of the department that owns the application
application will be the short name of the application itself
module will be the implementation section.

3.17 System Operations Domain

Principles

Data Center Operations provides first-line operational and virtual support and security (24-hours per day, 7-days a week) for mission critical servers, mainframe and main network hubs that reside in the County's Enterprise Data Centers. Major support services provided by the team include mainframe, server and Storage Area Network (SAN) operations, server backup/recovery, server hosting and system/network monitoring (NOC), and Data Production Control. Data Center Operations coordinates the Disaster Recovery plans and test exercises for several of the County's mission-critical systems. Operations protects the secured Data Center environments around the clock from power outages with UPS units and diesel generators. A constant climate controlled environment for the Data Centers is provided as well as fire protection and suppression systems. All hardware equipment is housed on a raised floor.



Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Data Center Operations Team.

Components

Data Center Operations Services:

Server Hosting/Co-location:

Server hosting and co-location services for Dell Intel, IBM mainframe, IBM & SUN midrange, and various appliances from DTS and other County Departments/Agencies. The County's main Network Hubs and voicemail system are located in the Data Centers. Physical security provided by card access only entry and closed-circuit video surveillance. 24x7 conditioned power uptime provided by a UPS unit connected to a diesel generator supplied by underground fuel tanks. All equipment is housed on a 12" raised floor and all rack cabinets are equipped with dual PDUs for power redundancy, and KVM over IP console switches for remote access. For network connectivity each rack connects to a Cisco switch configurable for accessing any segment on the County's network. Backup & monitoring is provided 24x7 for all equipment housed in the Data Centers.

Server Backup and Recovery:

The Data Center Operations team uses Symantec Veritas NetBackup v6.1. There is one NetBackup Master server that houses the main tape catalog and is where master scheduling and control is done. Communicating with the NetBackup Master are Multiple Media Backup servers with either LTO-2 or LTO-3 tape libraries attached to them. The Media Backup servers are located closer to the data that is going to be backed up and is where the data is physically backed up to.

Oracle database backups are exported to a file, which is then automatically picked-up by the nightly backups. Veritas's NetBackup Oracle and RMAN database agent is used for online backups of the Oracle databases. The Oracle database servers are connected to the Nexsan ATABeast or SATABeast disk arrays for disk-to-disk backups, which are also backed-up by the Veritas tape backup server.

Symantec Veritas Backup Exec v10 is also used for backups on various Windows based systems.

Backups are performed every day according to the following schedule:

- Daily (Incremental) - Monday thru Friday
- Weekly (Full) - Saturday
- Off-site (Full) - Sunday
- Monthly (Full) - 1st Saturday of each month

Server Backup Reporting provided by Aptare's StorageConsole v6.05

Monthly auditing of the server backups are performed by Operations and various server support teams.

Backup Retention Schedule

Backup	Retention Time
Daily	21 days (3 weeks)
Off-site (Full)	21 days (3 weeks)
Monthly (1st Weekend)	91 days (13 weeks)

Enterprise SAN Storage Management:

SAN Storage/Fabric Management & Operations of the County's Enterprise Dell/EMC CX500 Storage Area Network connected to a Connectix 1600 Fiber Channel Switch. Nexsan ATA/SATABeast SAN used for server hosting services and D2D backups and VTL (Virtual Tape Library) connected to QLogic 5202 Fiber Channel Switches. QLogic 2354 Host Bus Adapters (HBA) used by clients connecting to the various SAN configurations. SRM tool by Aptare is used for reporting purposes.

Network Operations Center (NOC):

Server, System & Network Monitoring of all systems located in the Enterprise Data Centers and various mission critical systems Countywide. CiscoWorks & WhatsUp Gold monitoring software used. Operations performs the coordination between Verizon & AMS for completing the trouble tickets on data circuits or switches involved.

Server Operations:

IBM mainframe operations support (see section 5.11 – Mainframe Application Services Domain), includes nightly production batch processing and printing. Staff provides server administrator assistance and the running of the nightly server backups. Operations maintains and runs the Laser Check printing system (Create-a-Check by Piracle) for the printing of the County's payroll checks and advices. Operations maintains an extensive online Procedures Manual.

Data Control:

IBM mainframe Production Control job scheduling using CA-7. Enterprise Job Scheduling using UC4 Global for all platforms (mainframe, windows, linux, unix). Currently MCtime is scheduled by UC4. Mainframe tape management using CA-1. Print output management and ERD/EOS support.

Off-Site Data Vaulting:

Daily off-site data storage vaulting of backup tape cartridges to the County's offsite data storage vendor, Monday – Friday. Emergency 2-hour tape callback available upon special request.

Facilities Management:

Data Center Infrastructure Management and monitoring. Includes electrical power, UPS, air-conditioners (cooling) and fire suppression system management. Card Access entry system and CCTV used for maintaining security of the Data Centers 24x7. Electrical branch circuit and room temperature monitoring is performed by Intellipool Network Monitor.

Hardware Used	Software Used
Dell Power Edge 2850 Dell Power Edge 1855 Blades	Microsoft Server, Redhat Linux
Dell PV132T LTO-2 Tape Library Dell PV136T LTO-3 Tape Library Dell MLM6010 LTO-3 Tape Library FalconStor VTL	Ipswitch WhatsUp Gold Aptare StorageConsole Falconstor IpStor
Dell/EMC CX500 Disk Array/SAN Dell/EMC B162 Fiber Switch Nexsan ATA/SATAT Beast Disk Array/SAN QLogic 5202 Fiber Switch	Veritas NetBackup Enterprise v. 6.1 Veritas NetBackup Oracle/RMAN Agent Veritas Bare Metal Restore v. 6.1 Veritas Backup Exec v10

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Microsoft Windows and Redhat Linux System Administration
Hardware Management and Troubleshooting
Veritas NetBackup Enterprise Administration and Setup
Veritas Backup Exec Administration and Setup
FalconStor IpStor Administration and Setup
SAN Administration and Setup
Veritas Bare Metal Restore Administration and Setup
Help Desk & Customer Service Skills
Basic Networking Skills

Standards and Guidelines

For the Microsoft Windows, Linux, and Sun Solaris platforms, the County's software standard for server backups is Veritas NetBackup Enterprise v. 6.1, and Veritas Backup Exec v. 10 as needed. LTO Tape Libraries containing 2 tape cartridge drives are attached to the backup servers. All server backup tapes are rotated off-site daily.

3.18 Team Collaboration

Principles

The Team Collaboration Service provides an easy to use online meeting place for internal county teams. Team members can come to a team portal and collaborate on projects using their desktop browsers. The collaboration service provides some of the following abilities to a team:

- Announcements
- Meeting Agendas
- Document Sharing
- Calendar
- Tasks
- Discussion Board
- Linking Ability

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

The County uses Microsoft SharePoint services for team collaboration. When a team requests a collaboration site DTS allocates an area on the Enterprise SharePoint server. DTS maintains the overall SharePoint server providing proactive server management and backup facilities. When a team requests a new site it is set up by the DTS SharePoint Administrator. The team must designate their own Site Administrator, who will be responsible for the content and administrative duties for the site, including:

- adding and deleting site users (Users must be county Active Directory members)
- management of the content

DTS will maintain a SharePoint section on the DTS departmental homepage on the Intranet Portal. The SharePoint section will contain information about the service as well as a directory of all SharePoint Sites.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Microsoft SharePoint Services
Team Collaboration
Windows Server
SQL Server

Standards and Guidelines

Collaboration Intake Form

A requesting team or department must fill out a Collaboration Service Request Form. The form contains:

- site description
- owning department
- administrator name
- group members (for initial AD group population)
- estimated project completion date

Collaboration Agreement

A requesting team or department must read and agree to the Collaboration Agreement. The Collaboration agreement lists roles and responsibilities for the service.

Extra Disk Space

The team environment will come with an initial amount of disk space.

Additional space required by the team will be allocated at a cost.

3.19 Configuration Management (CM) Tools

Principles

The Configuration Management Tools Service provides the following functions to a team:

- Version Control Code Repository
- Version Control Document Repository
- Requirements Tracking
- Bug Tracking
- Issues Tracking

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Server Team.

Components

The County uses two Open Source tools to provide the above services. The Version Control functions are provided through the Open Source Subversion Tool. The Requirements Tracking, Bug Tracking, Issue Tracking and the rest of the Application Lifecycle Management functions are provided through the Open Source Trac Tool.

The Subversion Tool is an Open Source follow on to the CVS product. It contains most of CVS's features and many enhancements. Requesting teams will be provided with a subversion project for their use.

The Trac Tool is an Open Source tool that provides requirement, issue and bug tracking to a development/deployment project. Also, the Trac tool provides such project management features as Milestone tracking, Version Timeline tracking, Regression test reports and Custom reports. It can have an interface to a Subversion project where code checkins can be linked to bug reports (and vice versa).

When a team requests one of the above services DTS allocates an area on the Enterprise CM Tools server. DTS maintains the overall CM Tools server providing proactive server management and backup facilities. When a team requests one of the new services it is set up by the DTS CM Tools Administrator. The team must designate their own CM Tools Site Administrator, who will be responsible for the content and administrative duties for the site, including:

- adding and deleting users (Users must be county Active Directory members)
- management of the content

DTS will maintain a CM Tools section on the DTS departmental homepage on the Intranet Portal. The CM Tools section will contain information about the services as well as a directory of all CM Tools sites.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Subversion
Trac
Linux
Apache/SQLite

Standards and Guidelines

CM Tools Intake Form

A requesting team or department must fill out a CM Tools Service Request Form. The form must contain:

- type of tool – repository and/or tracking
- site description
- owning department
- administrator name
- group members (for initial AD group population)
- estimated project completion date

Collaboration Agreement

A requesting team or department must read and agree to the CM Tools Collaboration Agreement. The CM Tools Collaboration Agreement lists roles and responsibilities for the service.

3.20 Enterprise Server Management

Principles

The Enterprise Server Management Service provides the following functions for management of both physical and virtualized Enterprise Servers:

- Availability Monitoring
- Inventory Management
- Configuration Auditing
- Performance Monitoring
- Event Management
- Historical Data Tracking and Reporting
- Incident Alerts and Escalations

Owners

Business Owner

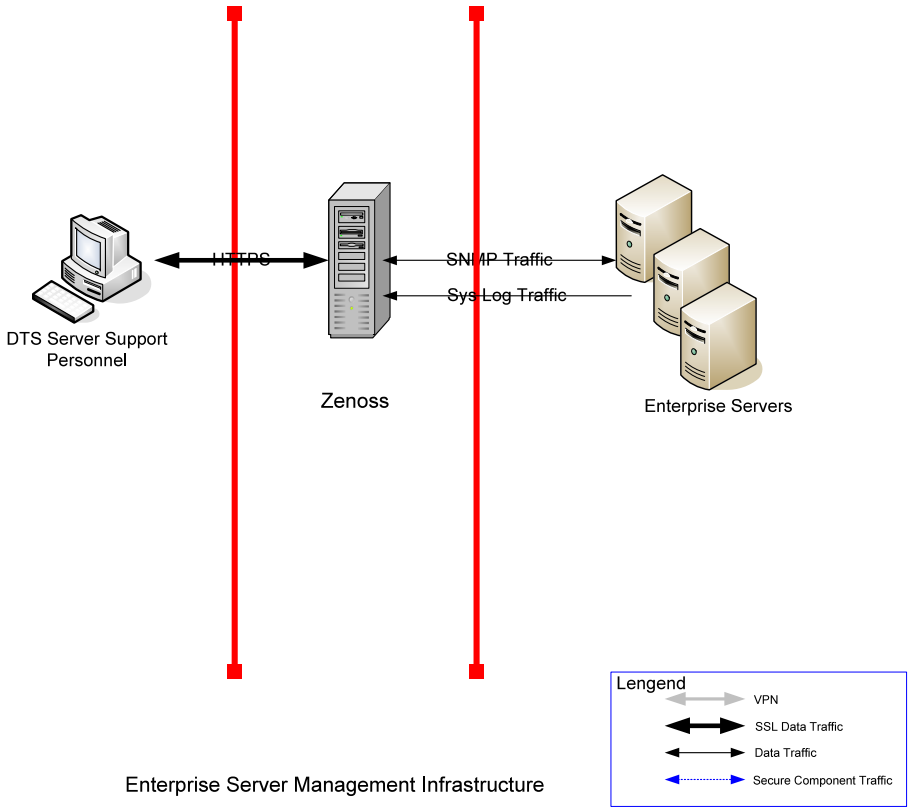
The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Server Team.

Components

Architecture Overview



Description

The County uses the Open Source Zenoss tool to provide the Enterprise Server Management Service functions to Enterprise Servers.

The DTS Server team runs an instance of Zenoss that has SNMP and SysLog access to the Enterprise Servers that the DTS Server Team manages. All physical and virtualized instances are modeled and monitored through the service.

Each server that is going to be modeled and monitored has its Syslog/EventLog and SNMP agent turned on in read only mode – sending the data ONLY to the Zenoss server. The Zenoss server is then provisioned by adding the server to its list of devices to model and monitor.

The Zenoss server is protected by a firewall with access to the server restricted to DTS personnel.

Functions

The DTS Server team uses Zenoss as its primary Enterprise Server Management tool. It uses:

- the monitoring and alert functionality through the use of the Zenoss console during business hours. Server team members respond to system alerts that identify performance and system issues
- the ITIL CMDB standard inventory capability of Zenoss for rich modeling of the servers and their Patch Management and Update process
- the performance monitoring capabilities for proactive alerts and capacity planning exercises
- the email notification capability to alert DTS Server Team Members performing off hours support of critical alert errors such as “System Down”
- various real-time and historical reports

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
SNMP, SysLog
Zenoss, Python

Standards and Guidelines

- All EHI physical and virtualized server instances are monitored. Beyond the server layer, no other devices (such as network appliance, backup servers) are modeled or monitored
- All MCGOV Internet and Intranet Portal Servers are monitored
- Only DTS Support personnel have access to the Zenoss Server (SSO Integrated)
- SNMP probes in monitored physical and virtual Server instances are configured as Read Only. They respond ONLY to the Zenoss server. SysLog probes also respond ONLY to the Zenoss server

3.21 Software as a Service (SaaS)

Principles

The SaaS Domain supports the use of externally hosted applications by Montgomery County. This service provides support that solves the common issues around using an externally hosted application. The common issues that are addressed within the SaaS support are related to:

- Identity
- Security
- Integration

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

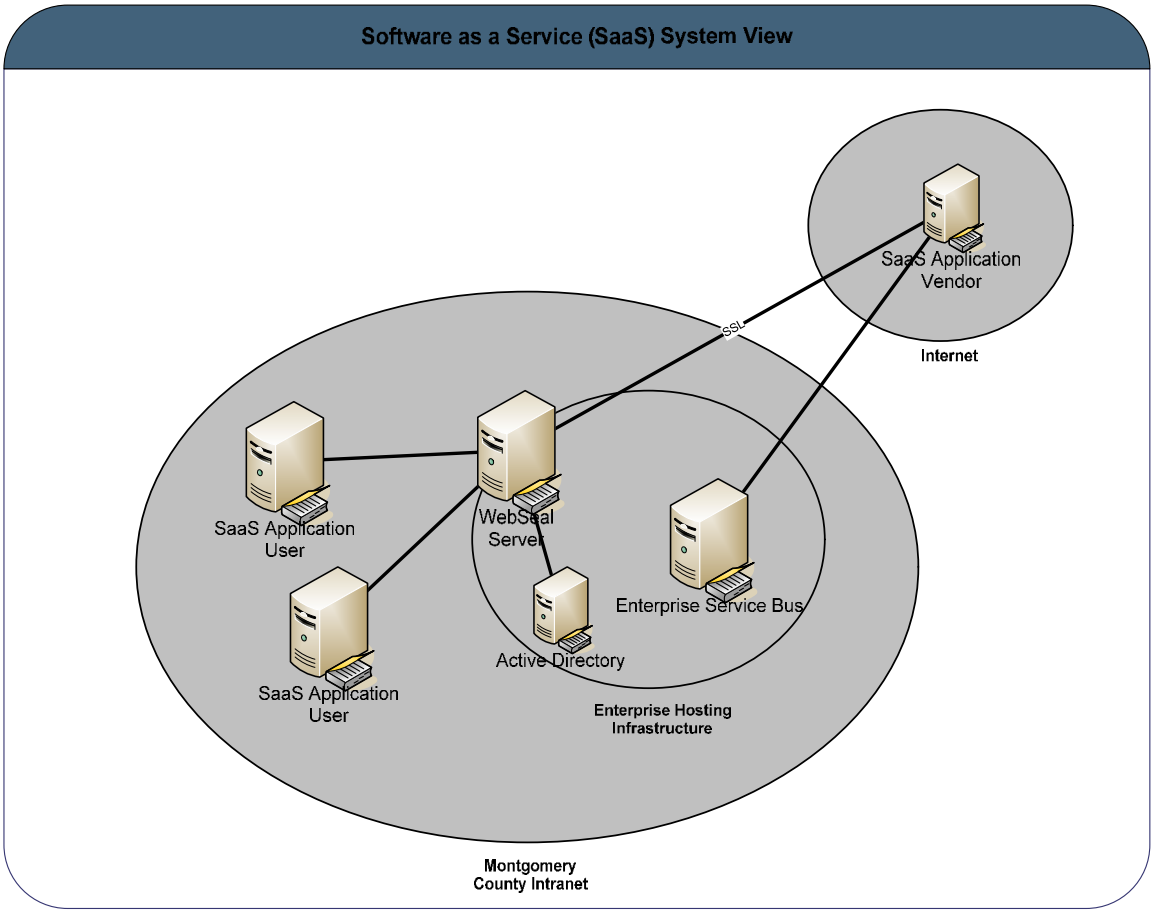
Technical Owner

The technical owner for this Domain is the DTS Enterprise Services Architect.

Components

The supported service makes use of the following IT Architecture Domains:

- Active Directory (AD) and Single Sign On (SSO) Services Domain
- Enterprise Hosting Infrastructure Domain
- Services Enabled Domain



Identity Services support centers around making use of the Active Directory (AD) and Single Sign On (SSO) Services Domain. It allows Departments to restrict access to the externally hosted application through the County Active Directory Domain. Users can be assigned to use the SaaS Application by the owning department through Active Directory.

Security Services support centers around the use of the Enterprise Hosting Infrastructure (EHI) Domain. The EHI is used as a front end to the externally hosted application. Once the user signs on through the normal county single sign on challenge an encrypted tunnel is opened out to the hosted application provider.

Integration Services support centers around the use of the Services Enabled Domain. The county's Enterprise Service Bus is used to securely pull data from the externally hosted application back into county systems or push the data to the externally hosted application from the county systems.

When a Department requests the above service DTS will work with the owning Department to identify the requirements around the application. They will work with the department and the vendor to roll out the service.

When a department requests the new service it must designate their own SaaS Application Administrator, who will be responsible for the content and administrative duties for the externally hosted application, including:

- adding and deleting users (Users must be county Active Directory members)
- being the coordinator and document/security key-owner of integration implementation(s)
- being the primary contact to the SaaS Application vendor

- management of the content

DTS will maintain a SaaS section on the DTS departmental homepage on the Intranet Portal. The SaaS section will contain information about the service as well as a directory of all SaaS sites.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Set
Active Directory Domain Administration
Windows 2003 Administration
TAM User Account creation
Understanding of Security Principles
Enterprise Service Bus (ESB)
Web Services

Standards and Guidelines

SaaS Intake Form

A requesting team or department must fill out a SaaS Service Request Form. The form must contain:

- name of the externally hosted application
- description of the externally hosted application
- vendor information on the externally hosted application
- owning department
- administrator name
- group members (for initial AD group population)
- description of data that must be retrieved from the externally hosted application back into the county
- destination where the retrieved data should go
- estimated retirement date for the application

Collaboration Agreement

A requesting team or department must read and agree to the SaaS Agreement. The SaaS agreement lists roles and responsibilities for the service.

The SaaS Application vendor must support an encrypted SSL tunnel from the county to the application.

The SaaS Application vendor must support static IP Addressing to it's service.

The SaaS Application vendor must refuse connections to the SaaS Application from sources other than the encrypted SSL tunnel from the county

If data within the SaaS Application is needed by the Department the SaaS Application must support retrieval of the data by the county Enterprise Service Bus.

If data that needs to be retrieved by the Department has a high confidentiality or integrity requirement than the SaaS Application must support encryption of the data and key based access to the data.

Recommendations

County Attorney's Office list of issues that need to be considered when procuring a cloud solution (not meant as an exhaustive list but as a starting point)

DTS recommends a Cost Benefit Analysis that includes the full life cycle of the solution and data

Owning departments are still responsible for County Discovery, Records Management, and Security and Privacy Policies

3.22 Database Hosting Infrastructure Platform

Principles

The Database Hosting Infrastructure (DHI) is the framework the County uses to deploy its enterprise databases. The County's DHI goals are to host Enterprise Databases in a standardized secure environment in a cost effective manner. The County benefits from DHI because its data is housed in a centralized manner that supports a centralized Data Architecture. Databases are documented with identified owners. Cost is reduced because the Data Owners benefit from the shared services offered by the Enterprise. The Shared Services not only includes the Database Servers but support services such as monitoring and backup.

DHI encompasses multiple components of the County's IT Framework: Deployment Domain, Network Domain, Security Domain, Help Desk, Active Directory & Single Sign On, and System Operations Domain.

When a new Database is targeted to be hosted in the DHI an intake form is filled out for the database. The intake form contains information about the database with one aspect of the information being the NIST Confidentiality, Integrity and Availability requirements for the application.

Confidentiality

"Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

A loss of confidentiality is the unauthorized disclosure of information.

Integrity

"Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542]

A loss of integrity is the unauthorized modification or destruction of information.

Availability

"Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542]

A loss of availability is the disruption of access to or use of information or an information system.

The county database standard supports both Oracle and Microsoft SQL Servers.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

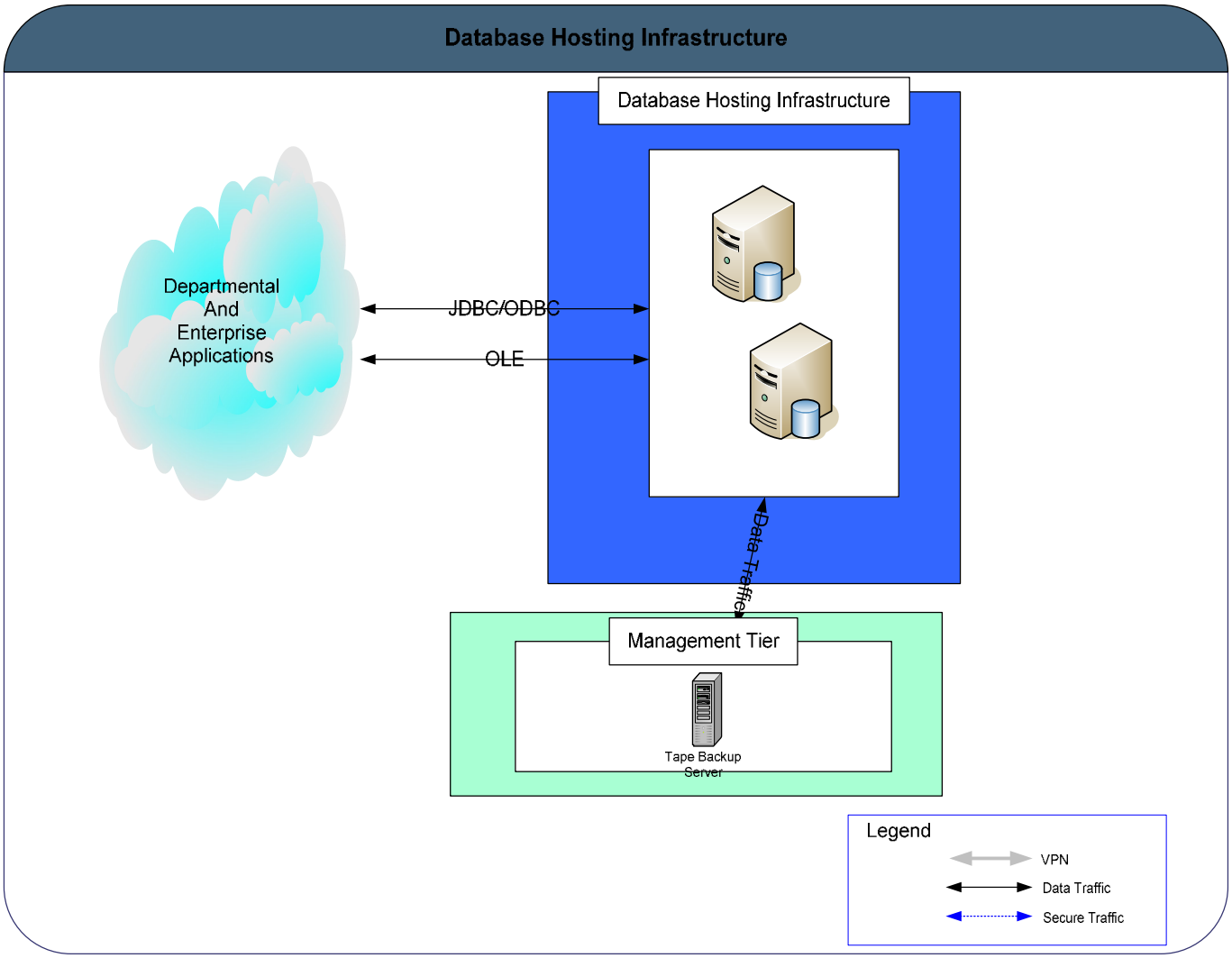
The technical owner for this Domain is:

- DTS Server Team

Components

Architecture Overview

In general, the DHI architecture is based on creating a security zone for just the Enterprise Databases. Access to the database servers is via ODBC/JDBC access only. It is a shared database server environment where multiple databases are hosted on the Enterprise Database Servers. Administrative access is kept within DTS with DTS delegating privileges to change and modify a user's database contents only. DTS does not give access at the database level or higher.


Database Hosting Infrastructure
Database Hosting Infrastructure
Departmental
And
Enterprise
Applications
JDBC/ODBC
OLE
Data Traffic
Management Tier
Tape Backup
Server
Legend
VPN
Data Traffic
Secure Traffic

Active Directory

Microsoft Active Directory is the master user registry for all county employees and for all applications hosted in the EHI (see section 3.1 – Active Directory (AD) and Single Sign On (SSO) Services). All LDAP traffic from the Web, Application, and Database tiers is encrypted (LDAPS) and accesses one of the Active Directory controllers. Active Directory also provides the primary DNS service for both Application and Database tiers of servers.

Database Server

The county supports both Oracle and Microsoft SQL servers under the DHI architecture. Users or Applications can access the database servers thru JDBC/ODBC/OLE.

Platform Choice

Hardware

All servers are Intel based and manufactured by Dell Computers. The hardware sizing is based on the County standard as outlined in the Deployment domain (see section 3.4 – Deployment Domain).

Operating System

Production Database Servers are all physical servers. Virtual Machines are not used.

The Operating Systems supported on the servers are:

- CentOS 5
- Microsoft Windows.

CentOS is an Open Source OS which uses the Red Hat Linux kernel and hence is an “identical twin” of Red Hat Linux.

The supported Microsoft Operating System is Windows Server.

Services

Backup Service

The DHI uses the backup services of the System Operations Domain. See section 3.17 – System Operations Domain for details.

Antivirus Service

Antivirus service is provided on the Windows Machines. Virus signatures are automatically synchronized from the county central Antivirus server.

Network

The DHI uses the Network Domain's Firewalls and Switches (see section 3.12 - Network Domain).

The DHI is separated from both the Intranet and the EHI through a stateful firewall. Internet access is not supported.

Security

Database Principles

The general principles that a database must follow are:

- Access to the Database must be through ODBC/JDBC only.
- Access to the Database from the Internet is not allowed.
- DTS solely has access and manages the production database servers.
- DTS delegates privileges to change and modify the database contents. DTS does not give access at the database level or higher.
- inactive session timeout
- Firewall is a stateful firewall

Standards

DHI Hosting Agreement

A requesting team or department must read and agree to the DHI Hosting Agreement. The DHI Hosting agreement lists roles and responsibilities for the database.

Administration Policies

- No access to the database servers other than by DTS employees performing administration services
- Monthly patching of Operating System and middleware software
- Virus updates every 10 minutes
- Daily backups
- Active Directory Group Policies (DTS Server Team Administrators are the only persons allowed to administer the machine and processes)
- Quarterly review of the Firewall Rules
- Quarterly review by Stakeholders of their database intake information
- Outage reports through HelpIT updates
- Maintenance window announcements through HelpIT updates

Database Hosting Intake Form

A requesting team or department must fill out a Database Hosting Service Request Form. The form

contains:

- Database Name
- Database Description
- NIST Security Classification for Confidentiality, Integrity, Availability (High, medium, low)
- Owning Department(s)
- Department(s) Administrators contact name
- Department(s) Administrators contact email
- Department(s) Administrators contact phone
- Department(s) Administrator Active Directory account
- Incident Response Plan
- Expected lifetime of the database

Physical Security

The networking switches and firewalls as well as the hosts that support the Production DHI are all located within one of the Department of Technology Services Data Centers (see section 3.17 – Systems Operation Domain).

Disaster Recovery

The DHI Domain involves the use of physical Deployment Domain Servers housed in the Data Centers in the System Operations Domain. DTS employs a number of disaster recovery strategies in the Deployment and System Operations Domains that essentially cover the following disaster scenarios:

- server loss
- rack loss
- data center loss

The server loss and rack loss strategy has a number of mitigation strategies within the System Operations Domain. Within the DHI Domain the mitigation strategies include:

- use of physical database server machines located in both data centers.
- in the event of individual server or rack failure critical databases will be moved to working database server machines
- in the event of a data center failure critical databases will be moved to working database servers in the other data center.

The design problem for the loss of one of the Data Centers is the prioritization of services that will be brought up in the working data center. See the Disaster Recovery Domain for information around prioritization of services and policies.

Help Desk Support

A key component of the DHI is the Help Desk (see section 3.9 – Help Desk Services). It provides a single point of contact for the users of databases hosted within the DHI. The Help Desk resolves problems or, as needed, routes problems to the DHI administrators.

As part of the intake process for a new DHI database a support plan is developed with the help desk. The support plan includes information such as:

- Identifying the business system owner
- Identifying the DHI Administrator contacts
- Identifying common problems and their resolution that a level 1 support person can handle
- Identifying the contact for level 2 problems

Server Administration

Administration of the DHI Servers is performed by the DTS Server Team (See section 3.20 – Enterprise Server Management)

3.23 Technical Disaster Recovery

Principles

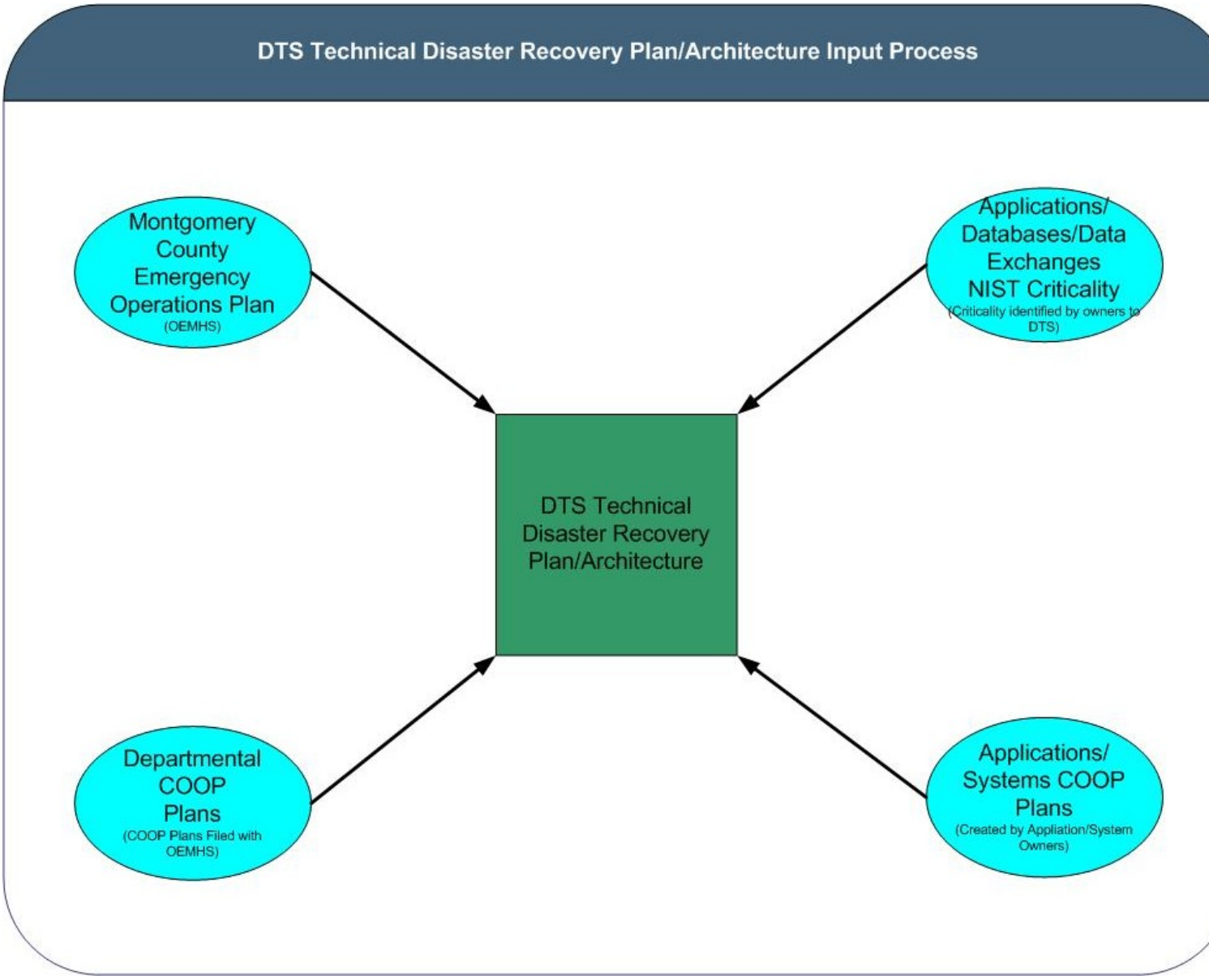
Disaster recovery is a complex undertaking that has both functional and technical components. It is strongly tied to COOP (process owned by OEMHS) and requires an iterative design approach with the business. It is not cost effective for the technical team to design a fully redundant Technical Disaster Recovery Plan and Architecture. A fully redundant plan requires a one for one replication of all services that have to be maintained and regularly exercised by both functional and technical personnel.

The Technical Disaster Recovery Plan and Architecture must work closely with the business to classify all business functions for criticality of operation. Questions that the business should ask itself are:

- How critical is the service?
- How long can it be down?
- Can data be lost? If so, how much?
- How much are you willing to pay? Initial expense? Yearly expense? Support extra functional and technical head count to regularly exercise and update the plan?

An effective Disaster Recovery plan must include use cases to help design and assess the Disaster Recovery plan. The use cases or scenarios help bound the problem and test the design.

The following graphic details the inputs to the Technical Disaster Recovery Plan and Architecture:



Disaster Recovery Strategy

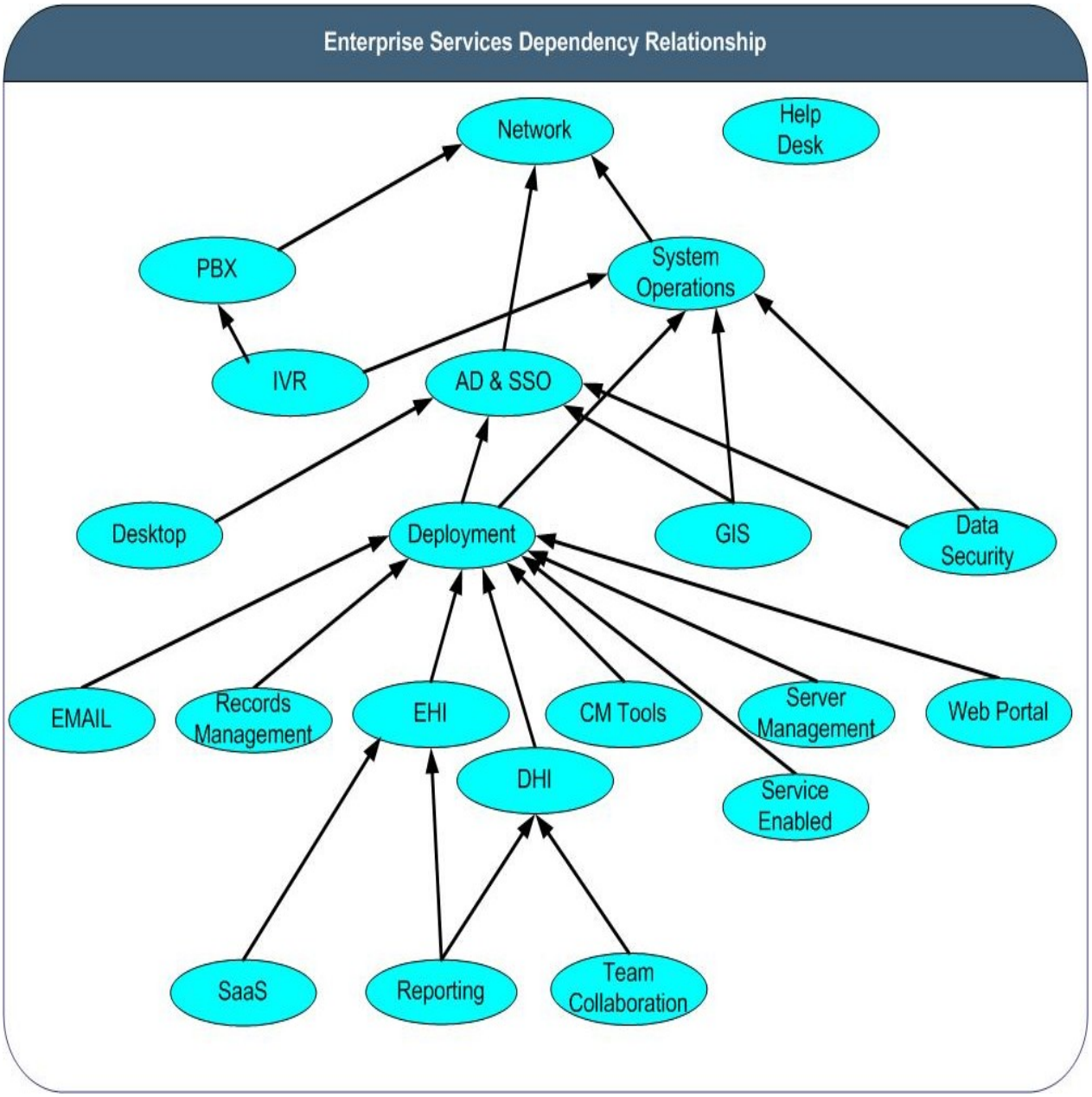
Technical Disaster Recovery is viewed from two perspectives. The first perspective involves the Enterprise Shared Services that are supplied to departments and agencies. The second involves the Enterprise and Departmental Services (applications, databases, and data exchanges) that are being hosted on the shared services infrastructures:

- Deployment Domain - VM Guests provided to departments
- EHI Domain - Enterprise Application Hosting
- DHI Domain - Enterprise Database Hosting
- Services Domain - Enterprise Service Bus (ESB) data exchanges

Enterprise Shared Services

The Department of Technology Services (DTS) offers a number of Enterprise Shared Services. Each one of the services is ranked in importance and the service includes as part of their Domain Architecture a section on Disaster Recovery that documents the processes and strategy for the particular service.

The Enterprise Services are built to work with each other and have the following dependency relationships:



DTS Hosting for Enterprise and Departmental Services

This section covers the hosted applications, databases, and data exchanges in the EHI, DHI, and the ESB.

EHI, DHI, and ESB

Applications, Databases, and Data Exchanges in the EHI, DHI, and ESB ultimately make use of the Deployment Domain. The Deployment Domain involves the use of VM Guests running on VM Hosting Servers housed in the Data Centers in the System Operations Domain. DTS employs a number of

disaster recovery strategies in the Deployment, Network and System Operations Domains that essentially cover the following disaster scenarios:

- server loss
- rack loss
- data center loss

The design problem for any of the three scenarios is the loss of VM Hosting Server capacity and the prioritization of services that will be brought up on the working VM Hosting Servers.

DTS will bring up services on the available capacity following the documented prioritization from highest to lowest **until capacity is exhausted**. DTS will bring up those services on the same IP address.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Server Team
- DTS Data Center Management Team
- DTS Core Team
- DTS Networking Team
- DTS PBX Team

Components

Architecture Overview

In general, the Technical Disaster Recovery Domain is based on the Disaster Recovery Sections in each of the component domains. The Disaster Recovery domain is essentially providing the overall guidance, governance, and the process.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
COOP Planning
Disaster Recovery Planning
Technical Services Redundancy

Technical Services Failover
Ability to use Magic Help Desk System

Standards and Guidelines

- Enterprise Services Domain's Disaster Recovery Components (see Disaster Recovery section in each service)
- Hosted Applications(EHI) , Databases(DHI) , Data exchanges (ESB) NIST Classification determines priority
- CIO assigns overall priority for both Enterprise Services and Hosted Services
- DTS declares the DR event
- DTS starts recovering services starting with the highest ranked services first
- Critical Departmental and Enterprise Solution COOP/Disaster Recovery plans
- Outage reports through HelpIT updates
- Data Center Recovery Plan
- Solution Level Disaster Recovery Services Agreement - A team or department that is requesting Solution Level Disaster Recovery Services must read and agree to the Disaster Recovery Service Level Agreement. The Disaster Recovery agreement lists roles and responsibilities for administering the service.
- Solution Level Disaster Recovery Services - Solutions and/or applications often use many interfaces and exchanges and require careful coordination. The Departmental or Enterprise Owners for an application should write a COOP/Disaster Recovery Plan for the application and work with DTS to provide a higher level of Disaster Recovery Services.

3.24 Enterprise File Services Domain

Principles

The County maintains a centralized Shared Enterprise File Service for use by Departments. A Department can request space on the Enterprise File Server(s) that are centrally managed by DTS. The Enterprise File Service is implemented on Microsoft File Servers and makes use of the Active Directory & Single Sign On Domain (see section 3.1) for security. A requesting Department is assigned a directory on the File Server and their administrator is assigned Administrator privileges for the directory. The Administrator has the ability to manage access and file privileges (ie Read/Write/etc).

Services provided to departments include:

- Centrally Managed Enterprise Shared File Service
- Ability to limit access to groups and individuals
- Ability to assign file permissions to groups and individuals
- Daily back ups via the Enterprise System Operations Domain

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

The Enterprise File Service is implemented on Microsoft Enterprise Servers within the Deployment Domain (see section 3.4). The Enterprise File Service is using the hosting and backup services of the System Operations Domain (see section 3.17) and is monitored and managed through the Enterprise Server Management (see section 3.20) Domain.

Requesting departments are assigned a Disk Space Quota that they are charged for and that DTS manages and monitors.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Active Directory Domain Administration
Windows 2003 Administration

Understanding of Security Principles
Ability to use Magic Help Desk System

Standards and Guidelines

Enterprise File Service Hosting Agreement

A requesting team or department must read and agree to the Enterprise File Service Hosting Agreement. The Enterprise File Service Hosting agreement lists roles and responsibilities for the service.

Administration Policies

- Root Access and Administrator privileges are limited to DTS employees performing administration services
- Monthly patching of Operating System and middleware software
- Virus updates every 10 minutes
- Daily backups
- Outage reports through HelpIT updates
- Maintenance window announcements through HelpIT updates
- Highly Recommended that each Administrator use Active Directory Groups for Authorization
- DTS Enterprise File Service Administrators will monitor capacity and notify departments when allocations are reaching maximum limits.
- Departments incur yearly charge backs for various disk quotas.

Disaster Recovery

DTS backs up Enterprise File Servers for disaster recovery purposes. DTS' current recovery process is to restore servers in the event of system crashes, facility loss, or some other disaster. To support the current model, Enterprise Backup tapes (see System Operation Domain) are retained 3 weeks. The Monthly (1st Weekend) backup is retained 13 weeks.

DTS will restore individual files from specific Enterprise file server backup tapes upon request.

3.25 Enterprise Print Services Domain

Principles

The County maintains a centralized Shared Enterprise Print Server for use by Departments. A Department can purchase a compatible printer either directly or through the DCM contract (see section 3.5 Desktop Domain) and have its profile and driver hosted on the Enterprise Print Server(s) that are centrally managed by DTS. The Enterprise Print Service is implemented on Microsoft Servers and makes use of the Active Directory & Single Sign On Domain (see section 3.1) as a directory service. A requesting Department will work with DTS to load their driver and profile on the Print Server. DTS will monitor and manage the centralized print queue. The owning department manages and maintains the printer.

Services provided to departments include:

- Centrally Managed Enterprise Shared Print Service
- Printers listed in a Directory Service (Active Directory)
- Central location for profiles and print drivers
- Authorized usage management
- Simple, local installation by end-user
- Printer firmware, driver updates
- Debug printer problems, interface with vendor
- Provide fax, imaging services
- Printer model compatibility with County's print server architecture

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owner for this Domain is the DTS Core Systems Team.

Components

The Enterprise Print Service is implemented on Microsoft Enterprise Servers within the Deployment Domain (see section 3.4). The Enterprise Print Service is using the hosting and backup services of the System Operations Domain (see section 3.17) and is monitored and managed through the Enterprise Server Management (see section 3.20) Domain.

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Active Directory Domain Administration
Windows 2003 Administration
Understanding of Security Principles
Understanding of Microsoft-based Enterprise printing
Ability to use Magic Help Desk System

Standards and Guidelines

Enterprise Print Service Hosting Agreement

A requesting team or department must read and agree to the Enterprise Print Service Hosting Agreement. The Enterprise Print Service Hosting agreement lists roles and responsibilities for the service.

Administration Policies

- Administrator privileges are limited to DTS employees performing administration services
- Monthly patching of Operating System and middleware software
- Virus updates every 10 minutes
- Daily backups
- Outage reports through HelpIT updates
- Maintenance window announcements through HelpIT updates

Disaster Recovery

DTS backs up Enterprise Print Servers for disaster recovery purposes. DTS' current recovery process is to restore servers in the event of system crashes, facility loss, or some other disaster. To support the current model, Enterprise Backup tapes (see System Operation Domain) are retained 3 weeks. The Monthly (1st Weekend) backup is retained 13 weeks.

3.26 Web Portal Domain

Montgomery County supports both Internet and Intranet web servers within the Web Portal Domain. The primary Internet Portal (www.montgomerycountymd.gov) is the main Internet (public access) entry point for County electronic government (eGovernment) services. The primary Intranet Portal (portal.mcgov.org) provides eGovernment services for County employees and associates (contractors, volunteers, partners, etc).

The Web Portal Domain is managed with a governance organizational structure that consists of a Change Control Board and an Oversight Committee. The Change Control Board, comprised of representatives from the Office of Public Information (OPI) and the Department of Technology Services (DTS), review, approve, or deny change control or policy, procedural and exception requests from County departments and agencies in accordance with the Web Portal Program Charter. The Oversight Committee, comprised primarily of representatives from the Office of the County Executive (OCEX), the County Attorney's Office (CAT), and key Department Directors or equivalents, creates, reviews, approves, and enforces County Web Portal Governance policies, procedures, and standards.

Montgomery County takes a decentralized approach to managing its web site. A small number of staff within the Department of Technology Services (DTS) and the Public Information Office (PIO), called the Core Web Portal Team, is responsible for designing, developing, testing, and maintaining Web Portal master templates, navigation menus / flows, and styles to support a robust information architecture and to maintain a web site continuity (County Brand), while providing greater flexibility, with regard to look and feel, and space "real estate". In addition, the Core Portal Team is responsible for designing, developing, testing, and maintaining a content management system (CMS) that enables designated non-technical web content contributors (editors) and administrators (approvers), dispersed throughout the County Government's departments and associated agencies, to create, maintain, and manage County Internet (publicly accessible) and Intranet (internal) web content in a secure and organized fashion with minimal training and simple, yet effective workflows. The CMS integrates with Internet and Intranet web content templates and leverages existing County information technology resources.

The Core Portal Team also reviews and recommends Internet and Intranet policies, standards, and practices to the Web Portal Change Control Board and Oversight Committee for their approval.

DTS maintains the Intranet and Internet (MCGOV) Web Portal Domains including County Web and Application Servers, Search Engine (Google) Servers, and Map Servers. In addition, DTS provides Intranet and Internet Server load balancing, incident response, and middleware support. Furthermore, DTS enforces access to the Web Portal Domains. File transfer access (read/write) permissions to the Web Portals are available through the County Content Management System (CMS) for web content and through JFM and/or an equivalent DTS approved tool for web applications.

While most County web content and web applications are hosted or stored on the Portal Servers, some departments (i.e. Department of Permitting Services, Department of Homeland Security and Emergency Management, and Department of Technology Services) own secondary web servers that are linked to and from the primary Portals. Secondary web servers are typically supported by the owning departments or offices and are approved by the PIO and DTS. Other servers currently within the Web Portal Domain are provided below:

Internet – Publicly Accessible Servers within the Web Portal Domain

- County Internet Application Server
  - www2.montgomerycountymd.gov
- Permitting Services Internet Server
  - permittingservices.montgomerycountymd.gov

- MC311
    - www3.montgomerycountymd.gov
- Geographic Information Systems (GIS) Map Server (Storm Operations)
    - www5.montgomerycountymd.gov
- GIS Map Server
    - gis2.montgomerycountymd.gov
- GIS Map Server
    - gis3.montgomerycountymd.gov
- Department of Transportation – Advanced Transportation Management System
    - atms.montgomerycountymd.gov
- Alert Montgomery – Office of Emergency Management and Homeland Security
    - alert.montgomerycountymd.gov
- Department of Recreation's RecWeb Site
    - recweb.montgomerycountymd.gov
- County Multimedia Web Server
    - stream01.montgomerycountymd.gov

Intranet – Employee / Associate Access within the Intranet Web Portal Domain

- Google Mini Search Appliance
- County Intranet GIS Web Server

The Internet and Intranet Portals can support various types of web content files, application programming languages and technologies, and multimedia file formats including, but not limited to the following:

Programming Languages and Technologies

- Adobe Shockwave Flash (SWF)
    - ActionScript /Flex
- Dynamic Hyper Text Mark-up Language (DHTML)
    - HTML, Javascript, and Cascading Style Sheets (CSS)
- Extensible Hyper Text Mark-up Language (XHTML)
- Extensible Mark-up Language (XML)
- Extensible Stylesheet Language Transformations (XSLT)
- Hyper Text Mark-up Language (HTML)
- Keyhole Markup Language (KML)
    - KML is used to specify a set of geo-spatial features (placemarks, images, polygons, 3D models, textual descriptions, etc.) for display in Google Earth, Maps and Mobile, or any other 3D earth browser (geo-browser) implementing the KML encoding
    - Typically compressed in Keyhole Markup Zip (KMZ) files
- Microsoft Active Server Pages (ASP)
- Microsoft Active Server Pages.NET (ASP.NET)
- Really Simple Syndication (RSS) 2.0
- Synchronized Multimedia Integration Language (SMIL or SMI)

Multimedia Files

- Adobe Flash Video (FLV)
- Adobe Shockwave Flash (SWF)
- Microsoft Windows Media Audio (WMA)
- Microsoft Windows Media Video (WMV)
- Moving Picture Experts Group - Layer 3 (MP3)

Web Content Files – Static

- Adobe Portable Document Format (PDF)
- Encapsulated Post Script (EPS)
- Graphics Interchange Format (GIF) – Image File Format
- Hyper Text Mark-up Language (HTML)
- Joint Photographic Experts Group (JPG) - Image File Format
- Microsoft Active Server Pages (ASP)
    - Used as the County's primary web content file format
    - Primarily consists of HTML
- Microsoft Office Files
    - PowerPoint (PPT), Excel (XLS), or Word (DOC, RTF, or TXT)
- Portable Network Graphics (PNG) – Image File Format
- Synchronized Multimedia Integration Language (SMIL or SMI)
- Tagged Image Format (TIFF)
- WinZip Files (ZIP)
    - Used to compress files for faster download speeds

The Web Portal Domain provides accessible web content and rich web applications featuring the following technologies:

- Web 2.0
    - County Information Center web applications enables users to subscribe to Really Simple Syndication (RSS) feeds and on-line newsletters, to read and interact with County Blogs, and to engage County leaders in on-line discussions
    - County On-Demand web applications provide access to web content (i.e. videos, news releases, etc..) using YouTube, Twitter, and Facebook technology
    - The Alert Montgomery System enables users to register to receive emergency alert text messages and notifications
    - MyMontgomery, an on-line mapping application integrated with Google Maps, enables users to find County service locations or places of interest (PLOI) by street address and zip code or by zip code only
- Web Accessibility
    - A dynamic text-only conversion function built into the County Web Portal templates enables screen reader browsers and other assistive technologies to access County web content (static)
    - A language translation web application uses Google's machine language translation tools to dynamically convert County web content into Spanish/Hispanic, Chinese, French, Korean and Vietnamese languages
- Web Content Discovery and Management
    - A semantic – friendly County Services Center web application / database is integrated with Google Site Search technology to enable users to quickly find on-line County services and information by keyword or phrase
    - A Content Management System is used to maintain and manage County Web Portal (Internet and Intranet) web content. Content providers are trained and encouraged to use descriptive links and page titles to improve content discovery

26.2 Owners

Business Owner

The business owner for this Domain is the Public Information Office.

Technical Owner

The technical owners for this Domain are:

- DTS Application Development and Integration Team
- DTS Server Team
- Public Information Office

26.3 Internet (MCGOV) Web Portal Domain

Principles

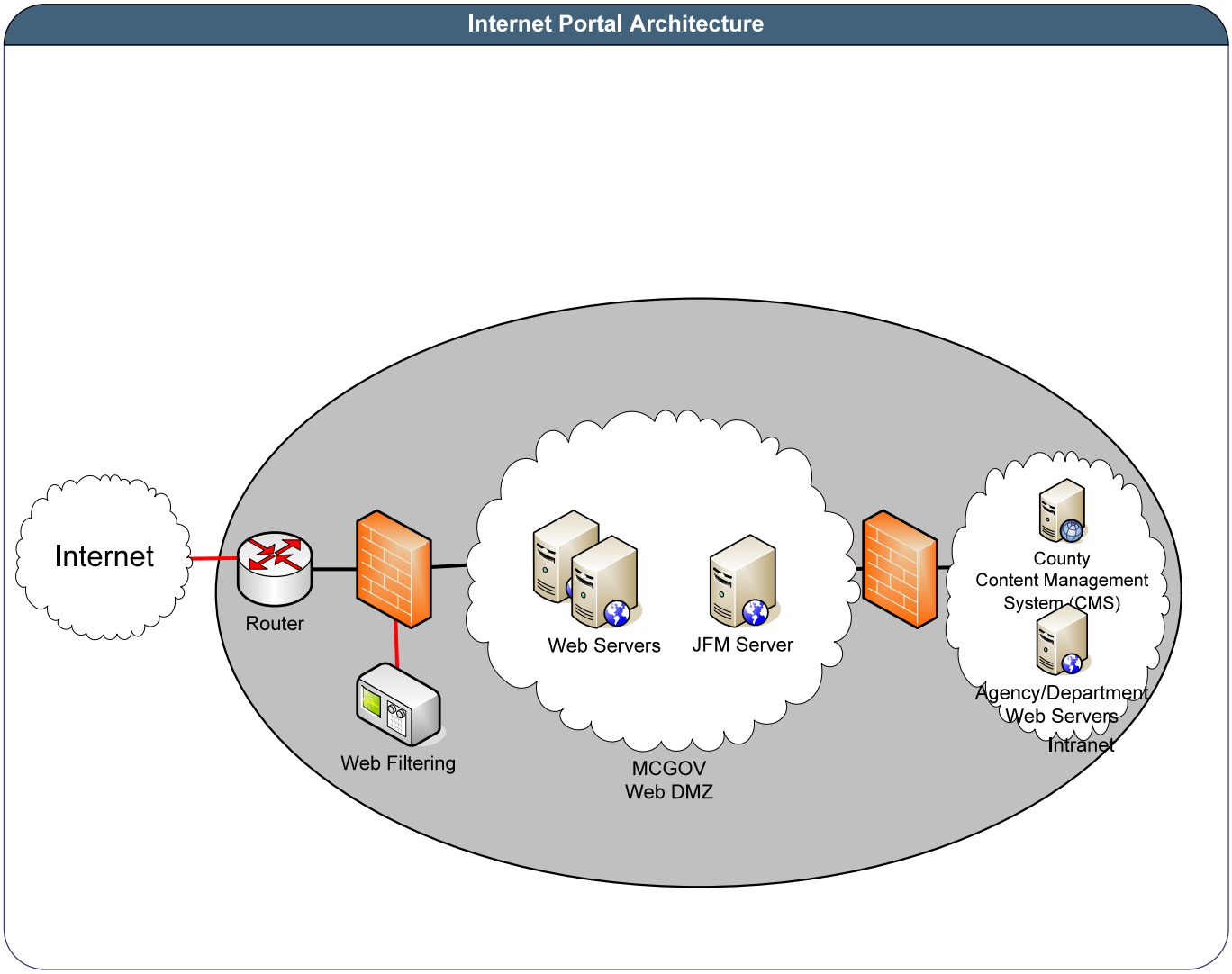
The audience for the Internet Portal includes, but is not limited to the following:

- County Residents and Visitors
- Other Government entities
- Business owners and operators
- Job seekers
- Other constituents

The publicly accessible web applications and content deployed on MCGOV Servers generally support the following functions:

1. Data Collection
    a. Recording or capturing data from constituents (i.e. registration for a meeting, survey, etc…)
    b. Enabling constituents to report an incident, event, etc… (i.e. pothole, street light outage, etc…)
2. Information Referral
    a. General query, results, and details information referral applications
    b. Interactive maps and travel directions (ArcGIS and Google map services)
    c. Multimedia streams (video and audio)
    d. Static web pages providing information referral services
    e. Web Services (i.e. street address validation)
3. On-line Payment Transactions
4. Subscriptions, Blogs, Interactive Messaging
    a. On-line newsletter and RSS feed subscriptions
    b. Blogs (Read-only)
    c. Message Boards (Live Discussion)
    d. Messaging (Emergency Alerts)

Components


Internet Portal Architecture
Internet
Router
Web Filtering
Web Servers
JFM Server
MCGOV
Web DMZ
County
Content Management
System (CMS)
Agency/Department
Web Servers
Intranet

Web Servers

The MCGOV DMZ consists of several Web Servers and includes links to publicly available applications running within the Enterprise Hosting Infrastructure (EHI) (See section 3.7 – Enterprise Hosting Infrastructure Platform). The Web Servers within the MCGOV DMZ are Dell Servers running Microsoft IIS Server and follow the Deployment Domain (see section 3.4 – Deployment Domain).

MCGOV – Internet Portal Server (www.montgomerycountymd.gov)

The Internet Portal (www.montgomerycountymd.gov) is used as the primary platform to deploy web content and applications to the public. A well-defined Internet Portal directory structure was created in a manner to enable application developers and content contributors to efficiently store and publish applications and content in addition to sharing common files. Content, Application, and Text Version Master Templates, which are used to provide web site design continuity (same look and feel) and flexibility (templates can be quickly altered to affect thousands of web pages), are stored in the County web site's root directory. In addition, County standard Content and Text master templates, written in traditional ASP, facilitate master template recognition (enabling relative link references), help to avoid content duplication (content can be assigned to multiple portals by link), address accessibility issues (content only converted to text on the fly), and interfaces with the Google Site Search Server.

Application master templates are available to County application developers in ASP and ASP.NET format. Code snippets are also provided in ASP master template common libraries or global files for application developers use to prevent common security vulnerabilities including web scraping (framing), SQL-Injections, and cross-scripting attacks. The proper use of the master templates by County application developers are enforced by the County Internet URL and Standard Design Template Policy. County Internet Privacy Policy, User Rights, Accessibility, and Disclaimer are provided for Portal visitors as well. The Internet Portal also provides a Secure Socket Layer (SSL) certificate for applications that require transmission encryption. Port 80 is the default open port using Hyper Text Transfer Protocol (HTTP). File transfer access (read/write) permissions to the Server is available through the County Content Management System (CMS) for web content and through JFM for web applications.

MCGOV – Internet Application Server (www2.montgomerycountymd.gov)

The Internet Application Server was created to store and serve ASP.NET web applications. The Server currently runs Microsoft IIS 6.x along with the ASP.NET Framework 1.1. and ASP.NET Framework 2.0 and consists of a directory structure that is similar to that of the Internet Portal Server. Application Server hosted applications are typically encrypted using Secure Socket Layer (SSL) certificate, thereby minimizing the risk in having Internet data transmissions intercepted or corrupted by unknown third party entities or hackers. Port 80 is the default open port using Hyper Text Transfer Protocol (HTTP). JFM can be used to deploy web applications.

Agency/Department Web Servers

Departments like Department of Permitting Services (permittingservices.montgomerycountymd.gov), Department of Homeland Security and Emergency Management (alert.montgomerycountymd.gov), and the Department of Technology Services (gis.montgomerycountymd.gov) have their own MCGOV Dell Web Servers. These departments typically have staff or contractors maintain and manage their servers, content, and applications. However, even though their applications and content are not hosted on the primary County Internet Server, the departments are expected to follow the County Internet URL and Standard Design Template Policy, unless they are granted an exception as specified in the Policy.

Content Management System (CMS)

The County CMS Server is housed in the data center (see section 3.4 – Deployment Domain and section 3.17 – System Operations Domain) and is the County's primary web content management system and repository. The CMS enables non-technical web content contributors or editors and publishers (approvers), dispersed throughout the County's departments and associated agencies, to create, maintain, and manage web content in a secure and organized fashion with minimal training and simple, yet effective workflows.

Authorization, Access, and Authentication

CMS users gain access to the system by opening the CMS URL using a Microsoft Internet Explorer web browser, entering their County Active Directory computer login user name and password, and selecting the web portal (Internet or Intranet) to update into the form provided. A user is authenticated using a County Active Directory and authorized, using a CMS SQL database, to edit content within their authorized and designated content directory and sub-directories. The CMS distinguishes between two types of users - those publishing the content and those approving it:

1. Content Editor
    a. A content editor can maintain and manage content, but does not have the ability to approve content to web portals
2. Content Approver
    a. An approver has the capability to maintain, manage, and approve content for publication on either web portal

A simple workflow has been incorporated into the system to enable content editors to submit content updates to their approvers or supervisors for review and approval. On request by an authorized County Content Manager or Department Director, DTS-ADT staff members update CMS application groups within the Active Directory – placing users in either Editor (User) or Approver group in order to allow them access to the CMS. Users may have permission to access both Internet and Intranet web content, but not during the same session.

Content File Management

After logging into the CMS, the file manager window opens and displays all of the folders and files within the user's authorized content directory. The file manager window enables users to navigate within their authorized content area, to access on-line help, and to perform content file management tasks. Users can use the file management buttons and links to upload or download multiple web or image files (pdf, html, asp, doc, gif, jpg, etc..), create or open new editable web content files or folders and to view, edit, rename, copy, delete, submit, or approve exiting content files or folders. Users can also determine web file's size (bytes) as well as the date and time it was last modified on the content server and last approved on its designated web portal. The CMS also allows all users to generate content freshness reports that provide a list of files, with their approval date and time stamps, that have been uploaded their respective web portals. User can then update stale content as necessary. The file manager also enables users to logout of their CMS session.

Content Editing

The user can either create a new content file to edit or edit an existing file listed in the CMS File Manager. Once a file, in .ASP or HTML file format, has been selected for editing, it is indicated as locked within the file manager and can not be opened by another content editor to eliminate any instances of more than one user editing the same page and overwriting another person's changes. The content editing tools enable users to edit web content text and assign County-approved web styles within their portal template content area (outlined with a blue box) without allowing them to edit the content master

template design or layout, which enforces County web design standards and policies. Each editable web content file contains HTML Comment tags identifying the content work area. The WYSIWYG content editor enables users to easily maintain or update text and insert, resize, and position images, tables, text boxes, or horizontal lines. CMS enables content editors to use the following word processing features:

- justify, center, and indent
- bold, italicize, underline, and bullet
- undo and redo text change
- spell checking
- find/replace, remove undesired text formats
- subscript and superscript
- insert special characters
- absolute positioning

In addition, the tool enables users to add and modify hyperlinks, mail links, anchors, page title and meta tags as well as saving, printing, previewing the web page in a another browser window. The CMS also enables users to view source code. Once the user has completed their edit session, they can save and exit the session in order to go back to the file manager window. They can also cancel the session without saving or by simply closing the web browser. When the browser window is closed, the system automatically ends the session and records that the session has ended. In addition, the CMS generates a session end courtesy message indicating that a session is about to end, thus providing a distracted user the opportunity to save their content and continue. If the content is not saved by the user prior to the session's end, the CMS saves the latest content version prior to closing the session.

Submitting and Approving Content to Selected Web Portals

Multiple content files can be submitted by the content editor to the Content Approver for review and approval. A CMS form enables the Content Editor to send a content update email message to their supervisor notifying them that web content changes have been made and that the content updates need to be reviewed. Once the supervisor receives the email, then he or she uses the CMS to review the updates and approve the content to either the Intranet or the Internet web portal. To approve the content, the Approver simply selects the content file(s) to approve and clicks the Approve and Upload button to update the selected Portal. The directory structure and files maintained on the content server match those found on the Internet and Intranet production servers. Consequently, the files are uploaded to their correct location every time. If the user creates a new folder, then the user need only approve the file within that folder and the new folder will automatically be created on the portal servers.

Java File Manager (JFM) Server

The JFM Server provides file transfer access to the Web Servers. Department users who have a special need to update their application content on the Web Servers can be provided access. They are provided access to their application folders on the Web Server and are restricted by privilege level to only their folders.

Google Site Search

The Google Site Search service provides sophisticated text-matching techniques to enable County Internet Portal visitors to quickly search and locate relevant web content by keyword or phrase. When a search is initiated by a user, the Google Site Search service searches all indexed web pages that contain all the keywords submitted. Basically, Google ignores common words and characters such as "where" and "how", as well as certain single digits and single letters, because they tend to slow down searches without improving results. In addition, Google searches are not case sensitive. If a search result cannot be found or is not relevant, then typically the web site visitor will refine their search by updating and resubmitting their search keywords or phrases to make them more specific.

Google Site Search is a cloud- hosted customizable search engine, built using Google's core search technology that enables the County to index 500,000 pages and to submit 3,000,000 search queries per year. County web site search forms, available in almost all County web pages, use Google Site Search technology to find relevant non-excluded content on a daily basis throughout the year. Google Site Search enables the County to crawl web servers / content outside of the County's firewall and currently indexes web page docs (html, htm, .asp, .cfm, .pdf, and .xml) and Microsoft Office file formats (.doc, .xls, and .ppt) from the following servers.

- http://www.montgomerycountymd.gov
- http://www2.montgomerycountymd.gov
- http://www3.montgomerycountymd.gov/mc311
- http://montgomerycountymd.libanswers.com
- http://montgomerycountymd.libguides.com
- http://permittingservices.montgomerycountymd.gov
- http://www.hocmc.org

Google Site Search department-specific search filters, refinements, and content weighing are available to County departments as well through Google Site Search.

Intranet Portal

Principles

The function of the Intranet portal is to support:

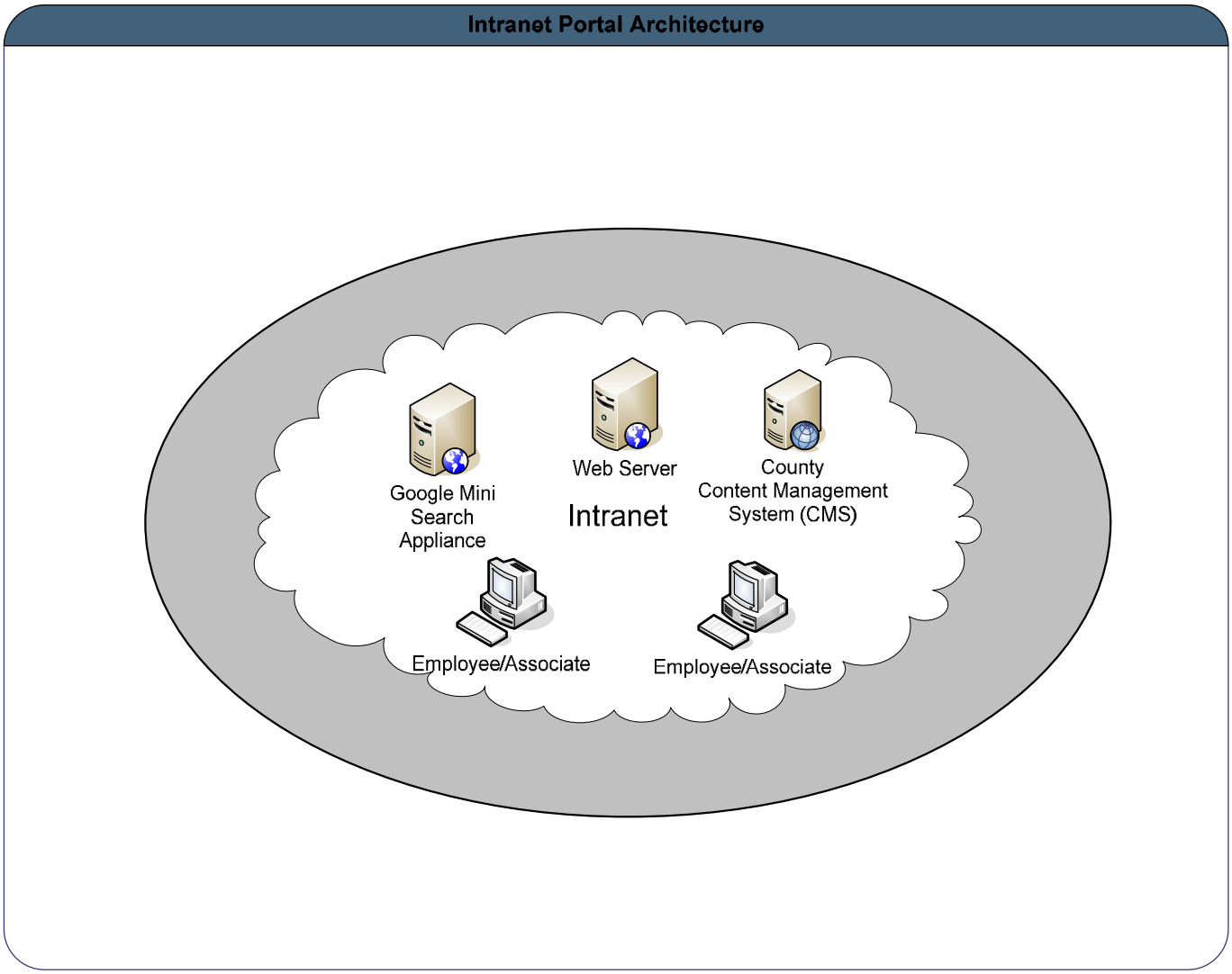
- Employee communications
- Employee services
- Departmental pages

The audience for the Intranet portal includes:

- Employees, Paid Interns, Temporary Workers (Active)

- Associates (Active)
  - Contractors
  - Partners - affiliated company/business user accounts, partners to the County
  - Volunteers - Volunteers, unpaid Interns

Components


Intranet Portal Architecture
Google Mini Search Appliance
Web Server
Intranet
County Content Management System (CMS)
Employee/Associate
Employee/Associate

Web Servers

The Intranet Portal is run on a single Web Server. The web server follows the Deployment Domain (see section 3.4 **–** Deployment Domain).

The Intranet Portal is a Dell Server running Microsoft IIS server and Cold Fusion Server as well as ASP.NET 1.1 and ASP.NET 2.0 frameworks. The Intranet Portal is used as the primary platform to deploy web content and applications (ASP, ASP.NET, and CFM) to County employees and associates within the work place and within the County Firewall. Much like the Internet Portal, a well-defined Intranet Portal directory structure was created in a manner to enable application developers and content contributors to efficiently store and publish applications and content in addition to sharing common files. As a result, static web content files are stored in the **Content** folder, dynamic web application files are published in the **Apps** folder, and commonly used files, such as scripts, images, and style sheets, are maintained in the **Common** folder relative to the web site's root directory. Content, Application, and Text Version Master Templates, which are used to provide web site design continuity (same look and feel) and flexibility (templates can be quickly altered to affect thousands of web pages), are stored in the Portal's web site's root directory (inetpub/wwwroot/). In addition, standardized master templates facilitate template recognition, help to avoid content duplication (content can be assigned to multiple portals by link), address accessibility issues (content only converted to text on the fly), and interfaces with the Intranet Google Mini Search Server.

Intranet application master templates are available to County application developers in ASP, ASP.NET, and Cold Fusion format. The proper use of the master templates by County application developers are enforced by the County Internet URL and Standard Design Template Policy. County Internet Privacy Policy, User Rights, Accessibility, and Disclaimer are provided for Portal visitors as well. The Internet Portal also provides a Secure Socket Layer (SSL) certificate for applications that require transmission encryption. Port 80 is the default open port using Hyper Text Transfer Protocol (HTTP). File transfer access (read/write) permissions to the Server is available through the County Content Management System (CMS) for web content and through JFM and/or an equivalent DTS approved tool for web applications.

Content Management System

See the Internet Portal section.

Google Mini Search Appliance

The Google Mini Search Appliance - M2 (search.mcgov.org), a rack mountable server (1U), combines Google's PageRank™ technology with sophisticated text-matching techniques to enable County Intranet Portal visitors to quickly search and locate relevant web content by keyword or phrase. The Google Mini supports a customizable interface that enables Intranet Portal template integration for search forms, search results, and advanced search results web pages. Consequently, web site visitors commonly enter a keyword(s) or a phrase, encompassed with quotes, within a County Intranet Portal template search form to quickly generate a search results web page presented within a County template.

When a search is initiated by a user, the Google Mini searches all indexed web pages that contain all the keywords submitted. Basically, Google ignores common words and characters such as "where" and "how", as well as certain single digits and single letters, because they tend to slow down searches without improving results. In addition, Google searches are not case sensitive. If a search result cannot be found or is not relevant, then typically the web site visitor will refine their search by updating and resubmitting their search keywords or phrases to make them more specific.

To improve the chances of content discovery, the Google Mini enables customized sub-site or department-specific search collections to be defined, thus, refining and improving the search results for advanced searches conducted within those collections. In addition, the Google Mini advanced web search options enable users to refine their search parameters by using a more detailed search form. Users can find results:

- By department-specific search filter listed in drop-down menu
    - Default Internet Portal Template search form includes all indexed Internet pages
- With all of the words
    - This is the default search setting
    - Search engine math equivalent (trash AND removal)
- With the exact phrase
    - inserts quotes around search keywords (i.e. "trash removal")
- With any of the words
    - Search engine math equivalent (trash OR removal)
- Without the words (i.e. trash removal -bins)
    - Search engine math equivalent (trash removal -bins)
- By Returning pages in various languages (Spanish)
- By Returning results where the search keyword or phrase is located:
    - Anywhere on the page
    - Within the page title
    - In the URL of the page
- By Only returning or not returning results from a specific web site or domain
- By Sorting by Relevance or by Date (descending)
    - Relevance is determined by Google algorithms (PageRank) and/or by user weighted values

The Montgomery County Google Mini Search Appliance – M2 currently enables search indexes of up to 100,000 web pages, including (Microsoft Office files, and PDF files). In addition, the Google Mini Administration tool enables administrators to configure, create, and schedule search collections, to schedule search exclude specified content from search crawls, to weight content to tune searches, and to generate keyword search reports. The Google Mini can be configured to search 220 different file formats

and automatically detects 28 different languages. In order for the Google Mini to crawl documents, the documents need to be web-enabled (i.e., accessible by HTTP or HTTPS protocol) or reside on networked file systems. The County's Google Mini currently "crawls" the primary Intranet web servers on a daily basis (scheduled crawl mode).

In-house Competency/Skill Set

To uphold a high level of service and component availability, DTS personnel are trained in key areas. These key area skills are listed in the table below.

Skill Set
Content Management
Web Development
User Interface Design
Database Administration
Microsoft IIS Server Management
Microsoft .NET Services
Microsoft IIS Server Security
Search Engine Administration
Training Skills
Technical Writing

Standards and Guidelines

Social Media

Interim Administrative Procedure 6-8, Social Media

Content

The following are general County Content Management standards and guidelines:

- **Performance Guideline**
    - The County expects a turn around time for Web content in 3 seconds or less
- **Availability Guideline**
    - The County expects Web content to be available no less than 99.5% of the time
    - The County expects the CMS to be available no less than 99% of the time
- **Content Management Standards, tutorials, frequently asked questions, workflow diagrams, and user group presentations**
    - Available on DTS Intranet Web Site (http://portal.mcgov.org/content/departments_intranet/dts/Resources/WEP/index.asp)
- **Web Content Management User Group Blog (available on Intranet Web Site)** http://portal.mcgov.org/apps/News/Blog/IntraGenericBlog.asp?blogID=5&Cat=web%20policy

- Information Architecture
- Usability Studies
- Policies, Procedures, and Design Standards

- **County Internet URL and Standard Design Template Policy**

  Naming Convention Syntax Examples:

  - Internet Primary Portal
    - www.montgomerycountymd.gov/content/<<dept>>/sub-folder(s)/ web page
    - www.montgomerycountymd.gov/content/<<dept>>/web page
    - www.montgomerycountymd.gov/content/<<portal>>/sub-folder(s)/ web page
    - www.montgomerycountymd.gov/content/<<portal>>/web page
  - Intranet Primary Portal
    - portal.mcgov.org/content/<<portaldirectory>>/<<dept/project>>/web page
    - portal.mcgov.org/content/<<portaldirectory>>/<<dept/project>>/sub-folder(s)/ /web page
  - Syntax Definitions
    - portaldirectory = Intranet portal directory (i.e. departments_intranet)
    - dept = short name of the department that owns the application

- **Shortcut and Accessibility Standards**

Applications

See the MCG Enterprise Architecture Application Architecture document.

3.27 Mobile Computing Domain

Principles

The Mobile Computing Domain provides support for Mobile Client devices such as smart phones, netbooks and tablets. It is an extension of the Desktop (DCM)(see section 3.5), Network (see section 3.12), and Data Security domains (see section 3.3).

With the advance in intelligence of non-traditional mobile computing devices the County has found the need to support these devices for County Mobile User populations and as secondary devices.

The user populations for this domain are expected to include:

- traditional seat machine for mobile users where the seat machine is a device such as a tablet or netbook
- secondary or user owned personal devices employed as productivity aids

Support comes in two categories that correspond to:

- behind the fire-wall devices
- outside the fire-wall devices

Mobile device support that is behind the firewall is for County owned devices that can meet County Security and management policies. This support means that they can access the internal County wireless network through the Wireless Access security protocol (see section 3.12 Network Domain for details). The Mobile Device is considered a County Device that is owned by the County and is centrally managed in an inventory system, has a standard image, can be managed through a remote login service, and is using the Enterprise Virus Protection Services (see section 3.3 Data Security Domain for details). Devices such as these are acting as seat machines and are supported through the help desk and DCM replacement schedule like a DCM desktop or laptop.

Mobile device support that is outside the firewall can include County Owned devices purchased through the DCM contract as well as personal devices. These devices operate outside the internal County network. For these devices the County offers limited County Application support that includes Internet access for applications like:

- MCTime (timesheet)
- County Email and Calendaring (see section 3.6 Email System Services)
- ERP Employee self-service

The device must support the particular Application's Web Browser Requirements.

Additionally, the County VPN offers limited support for mobiles that can allow them to log in to the internal County network and access certain behind the fire-wall services.

Owners

Business Owner

The business owner for this Domain is the DTS CIO.

Technical Owner

The technical owners for this Domain are:

- DTS Client Computers (DCM) Team
- Security Team (VPN)
- Network Team

Components

Mobile Device

The mobile device can be any mobile device that meets VPN access requirements or the browser requirements of the externally offered applications.

County owned devices are possible either as a seat machine offered through the County DCM contract or as a departmental purchased system that can be bought through the DCM contract but is not a seat machine.

Network Access

All personal and non-centrally managed devices must access County Services outside the internal County network. The Network Team is planning to upgrade current County wireless access points to support both internal County network access as well as external access. External access will tunnel the device out to the County external Firewall where they can access County Internet based services or use the VPN to access the internal County network.

Application Support

The County Email and Calendaring system (see section 3.6 Email System Services) supports Internet access via OWA. Other application owners can chose to make their application available externally by hosting them in the Enterprise Hosting Infrastructure (see section 3.7 Enterprise Hosting Infrastructure Domain). These applications can support mobile devices if the mobile device browser can meet the EHI and Application minimum requirements.

Security (VPN)

The DTS Security Team maintains a VPN (see section 3.3 Data Security Domain for details) and is the primary solution for external users to gain access to the County internal network. Users must be approved for the VPN and use a device that is supported by the VPN. Upon login all devices are checked for up to date Operating Systems and for certain class of machines for up to date Virus checking software and definitions.

In-house Competency/Skill Set

To maintain the architectural components, DTS personnel are trained for proficiency in specific areas. These skills are listed in the following table.

Skill Sets
Desktop Computer Management
Tablet, Netbook, and Smartphone administration
Virtual Private Networking Administration
Network Access Point Administration
Enterprise Application development and support.

Standards and Guidelines

- Service Level Agreement (SLA) for Mobile Device Support under Desktop Computer Modernization (DCM) Program
    - SLA for departments using mobile devices

- Office of Management and Budget – Administrative Procedure 6-1 *Use of County-Provided Internet, Intranet, and Electronic Mail Services*

- Office of Management and Budget – Administrative Procedure 6-6 *Information Technology Policies and Procedures*

- Office of Management and Budget – Administrative Procedure 6-7 *Information Resources Security*

- Office of Management and Budget – Administrative Procedure 8-2 *HIPAA Compliance and Responsibilities*